



U.S. Department
Of Transportation
**Federal Aviation
Administration**

SOC

Safety Oversight Circular

SOC 08-07
Date AUG 20 2008

Air Traffic Safety
Oversight Service (AOV)

Subject: Guidance Regarding the Validation and Verification of the ATO Safety Management System

1. REFERENCED DOCUMENTS

- FAA Order 1100.161 *Air Traffic Safety Oversight Service*
- ICAO Document 4444 *Air Traffic Management (PANS-ATM)*
- ICAO Annex 11 *Air Traffic Services*
- Air Traffic Safety Oversight Service Memorandum ATO Vice President of Safety Services, *ATO Safety Management System Requirements*, August 24, 2005.

2. PURPOSE

This Safety Oversight Circular (SOC) provides general information and guidance regarding the methods and standards by which the Air Traffic Safety Oversight Service (AOV) will conduct its Validation and Verification (V&V) of the Air Traffic Organization (ATO) Safety Management System (SMS). This information is provided in order to help prepare ATO for the V&V process.

3. BACKGROUND AND DISCUSSION:

- a. Under FAA Order 1100.161 *Air Traffic Safety Oversight Service*, ATO must “develop and maintain a Safety Management System (SMS) and submit it and any changes thereto, to AOV for approval.” AOV, in turn, is responsible for establishing requirements for the ATO SMS “in accordance with International Civil Aviation Organization (ICAO) Annex 11 to the *Convention on International Civil Aviation, Air Traffic Services*, and ICAO Document 4444 (ATM/501), *Procedures for Air Navigation Services, Air Traffic Management*”. Approval of the ATO SMS is accomplished via a system engineering process called “Validation and Verification”. V&V confirms that system requirements are correct (validation) and satisfied (verification).
- b. Specifically, validation involves an evaluation to establish that the ATO SMS completely, consistently, and unambiguously reflects relevant Federal Aviation Administration (FAA) and ICAO requirements. Inconsistencies identified by AOV evaluations are documented for corrective action by ATO. Relevant FAA requirements are found in the following documents:

- FAA Order 1100.161 *Air Traffic Safety Oversight Service*
 - Air Traffic Safety Oversight Service Memorandum ATO Vice President of Safety Services, *ATO Safety Management System Requirements*, August 24, 2005
- c. Once ATO SMS requirements are complete and consistent with FAA and ICAO requirements, verification then establishes that the ATO SMS requirements are correctly implemented. In broad terms, verification ensures that the system requirements have been met by the design solution and that the system is ready to be used in the operational environment for which it was intended. In accordance with the basic organization of a safety management system, the AOV verification process divides these requirements into the following four areas:
- Safety Policy
 - Safety Risk Management
 - Safety Assurance
 - Safety Promotion
- d. In theory, the V&V process extends to all levels of an organization, although in practice the lowest (most disaggregated) levels are evaluated through a sampling procedure. Figure 1 shows a “multi-*V*” illustration of the V&V process. In the “*V*” representation, the left and right arms of each “*V*” represent validation and verification components, respectively. The largest “*V*” encompasses the organization as a whole, including individual facility SMS; the smaller “*V*s” represent different levels of the organization.

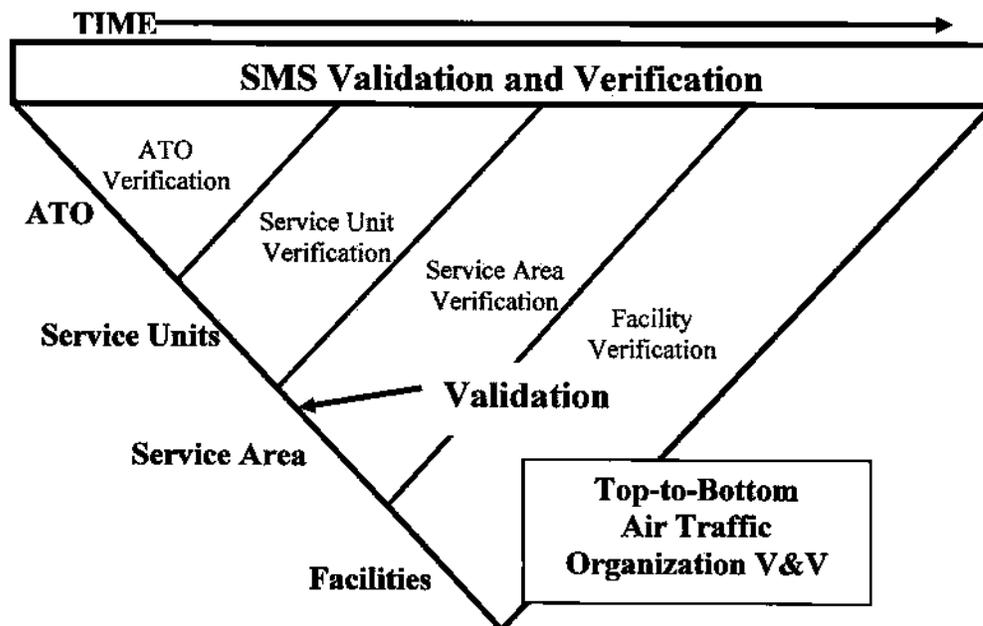


Figure 1. “Multi-*V*” Diagram Representation of ATO SMS Validation and Verification

Figure 1 also shows the general time sequence of the V&V process with the highest level requirements evaluated first, followed by successively lower levels of the ATO. In this way, the V&V process confirms that the highest level requirements are appropriately translated to the lowest levels of the organization. For example, facility V&V sampling could include an

evaluation to determine that facility operating procedures are consistent with ATO SMS requirements.

- e. AOV is committed to continual engagement with the ATO in order to maximize the likelihood of successful SMS implementation prior to the target date of March 2010. This is evidenced by the fact that V&V activities have been underway for several years. In May 2004, AOV granted ATO interim approval of the SMS, as documented in the SMS Manual Version 1.1. In a memorandum dated June 23, 2004, AOV requested that the MITRE Corporation Center for Advanced Aviation System Development (CAASD) provide an independent validation assessment of the SMS Manual. The results of the assessment were used to provide feedback to ATO on the strengths and weaknesses in its SMS design. In the same spirit, this SOC provides broad direction to ATO in advance of the target SMS implementation date.

4. DISPOSITION:

This guidance does not constitute a change to any requirement contained in FAA orders, manuals, etc. However, applicable Standard Operating Procedures (SOP) should be changed to reflect the processes defined in this SOC.

5. GUIDANCE:

a. Summary of AOV Validation and Verification Process

As described in paragraph 3 of this SOC, V&V activities will begin with examination of aggregate ATO-level requirements and continue to lower levels of the organization including facility-level sampling. The process is summarized in figure 2.

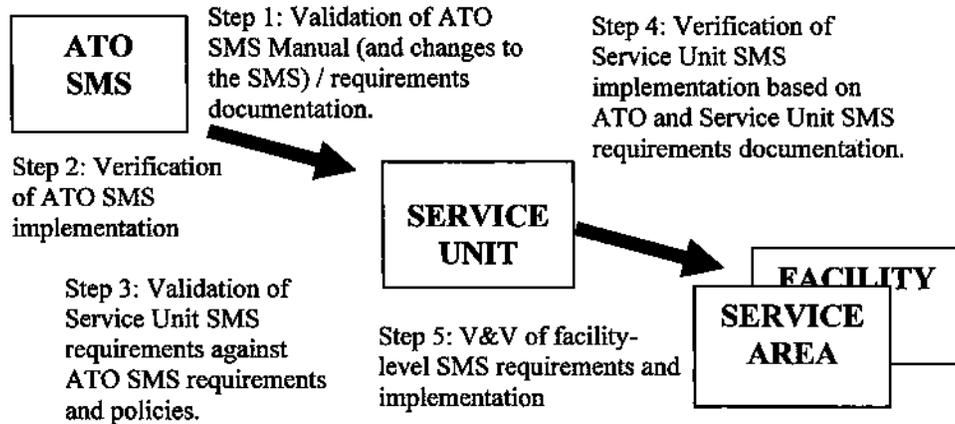


Figure 2. Summary of AOV V&V Process

1) Step 1: Air Traffic Organization Validation of Requirements

At the ATO level, validation will begin with an evaluation of the ATO Safety Management System Manual (ATO SMS JO 1000.37) and SMS implementation plan as they relate to relevant FAA and ICAO SMS requirements. In accordance with FAA Order 1100.161, paragraphs 2-1.e and 2-2.b, the SMS Manual (and changes to the SMS Manual) will be approved by AOV.

2) Step 2: Service Unit Validation

Upon validation of ATO SMS requirements, the next step in the V&V process involves an assessment of whether ATO requirements have been appropriately translated into ATO service unit implementation plans for:

- Acquisition and Business Services, Communications
- En Route and Oceanic Service
- Operations Planning, System Operations Services
- Technical Operations Service
- Terminal Service

Service Unit level validation involves a detailed analysis of Service Unit SMS documentation (e.g., Orders, SOPs, etc.) against ATO SMS requirements.

3) Step 3: Service Unit Verification

Verification refers to the analysis which determines whether ATO-wide and Service Unit SMS requirements have been correctly implemented. This analysis will be conducted through AOV audits of Service Unit safety management systems and implementation plans.

4) Step 4: Service Area and Facility V&V

V&V must extend to the level at which ATO interacts with customers at the point where service is provided. This will be done by auditing service areas and facilities in order to evaluate:

- (i) how well service center and facility SOPs conform to ATO SMS requirements
- (ii) how well SOPs relating to SMS are being followed
- (iii) how airspace changes are processed and approved
- (iv) how safety risk is managed

b. Summary of FAA SMS Requirements

As discussed in paragraph 3, the AOV V&V program can be divided into four components, reflecting the standard SMS organization: Policy, Safety Risk Management, Safety Assurance, and Promotion. The table below enumerates the requirements for each of the four components, and provides examples of the information that would be required for V&V.

1) Safety Policy Requirements.

Requirement Citation	Requirement Description	Examples
FAA 1100.161 3.3 a4	Development of minimum National Airspace (NAS) service level availability requirements, which include validation and verification of these requirements, for new systems entering the NAS and hardware and/or software improvements to existing systems.	Establish minimum NAS service level availability requirements and the NAS service level availability requirements for new systems. Verify and validate NAS service level availability requirements for new systems and system improvements before their entry into the NAS.
<i>ATO Safety Management System Requirements</i> Memo, SMS 1.0	The ATO shall implement a Safety Management System (SMS) that provides for a systematic approach to safety and establishes an effective organization to deliver and monitor safety performance.	
SMS 1.01	The Chief Operating Office (COO) shall be responsible and accountable for safety of the NAS, and shall ensure that all levels of management within the ATO are held accountable for ensuring that required safety levels are maintained in the provision of air traffic services.	Document policies regarding NAS safety and ensure compliance with policies on NAS safety. Hold top management accountable for safety.
SMS 1.02	Clear and unambiguous lines of authority and responsibility for SMS compliance shall be established and maintained at all organization levels and within all service units.	Clear and unambiguous lines of authority and responsibility for SMS compliance are visible to all employees through guidance and training.
SMS 1.04	ATO shall promote and measure SMS implementation and performance.	Provide personnel incentives for SMS implementation and performance. Measure the success of these incentives through periodic audits.
SMS 1.06	ATO shall establish an ATO Safety Unit responsible for developing, implementing, and maintaining the SMS.	Establish a Safety Unit. The Safety Unit is responsible for developing, implementing, and maintaining the SMS.
SMS 1.07	The Safety Unit shall be organizationally independent from the service delivery portion of ATO.	Establish a Safety Unit that is organizationally independent from the service delivery portion of ATO.
SMS 1.08	At each organizational level, the safety manager shall report directly to the general manager of that organization.	The safety manager is on the manager's first level staff and participates in the management of the organization.

2) Safety Risk Management Requirements

Requirement Citation	Requirement Description	Examples
FAA 1100.161 2.2.f	Provide to AOV regular and periodic (as set by AOV) status briefings, to include information regarding NAS changes being tracked by the ATO Safety Unit. The NAS change tracking data will be developed. ATO compliance with this reporting requirement will be effective September 15, 2006.	Provide status briefings to AOV regarding NAS changes being tracked by ATO-S.
FAA 1100.161 2.2.g	Develop and maintain a hazard tracking database in which all types of medium and high risk hazards are tracked, and provide continuous AOV access to the database. ATO compliance with this reporting requirement will be effective September 15, 2006.	Enter and track medium and high hazards in a hazard tracking database and provides means to track, manage, resolve, and communicate hazards. Grant AOV access to this database.
SMS 1.03	The ATO shall develop, implement, and maintain written SMS instructions and procedures for conducting safety management.	Implement written Safety Risk Management (SRM) instructions and procedures and maintain these written SRM instructions and procedures
SMS 1.05	The ATO shall comply with established safety standards and the approved procedures and standards contained in the approved SMS.	Comply with established safety standards and the approved procedures and standards contained in the approved SMS.
SMS 2.0	The ATO shall document the acceptable level of safety risk applicable to the provision of air traffic services. The acceptable level of safety risk may be specified in qualitative or quantitative terms.	Define and follow a process to monitor, adjust, and improve the specified acceptable level of safety risk.

Requirement Citation	Requirement Description	Examples
SMS 2.01	The SMS shall define a risk matrix depicting acceptable and unacceptable risk.	Define a risk matrix depicting acceptable and unacceptable risk.
SMS 2.02	The SMS shall define both elements of risk: severity in qualitative and likelihood in both quantitative and qualitative terms.	Define severity in qualitative terms. Further, define likelihood in both quantitative and qualitative terms.
SMS 3.0	The ATO safety management system shall include Safety Risk Management (SRM).	Describe SRM in the ATO SMS Manual and other safety guidance materials.
SMS 3.01	The ATO SMS shall identify actual and potential hazards.	Follow guidelines and requirements to properly identify potential hazards through a standardized and documented SRM process.
SMS 3.02	The ATO SMS shall assess the risk of those hazards.	Assess the risks associated with identified hazards according to SMS guidelines.
SMS 3.03	The ATO SMS shall determine necessary mitigation of those risks to an acceptable level.	Determine the necessary mitigations of the hazards to an acceptable level.
SMS 3.04	The ATO SMS shall verify that the mitigations are included in the system.	Identify and verify Mitigations before implementation.
SMS 4.0	Any change to the NAS, whether or not a Safety Risk Management Document (SRMD) is developed, shall only be implemented after a safety assessment has demonstrated that the change will meet or exceed the defined acceptable level or safety risk.	
SMS 4.01	ATO shall establish a framework for identifying, monitoring, and documenting proposed NAS changes.	Establish a framework for identifying, monitoring, and documenting proposed NAS changes.
SMS 4.02	NAS changes with identified actual or potential hazards shall be subject to the provisions of the SRM as required in SMS 3.	
SMS 4.03	All decisions determining that NAS changes do not have identified actual or potential hazards and therefore are not subject to the provisions of SRM must be documented in a written statement that includes a description of the decision and supporting documentation signed by a manager and kept on file for a period equivalent to the lifecycle of the system or change.	Document, in a written statement, decisions that includes a description of the decision and supporting documentation signed by a manager. Keep these documents on file for a period equivalent to the lifecycle of the system or change.

	All activities undertaken in an ATO safety management program shall be documented. All documentation shall be retained for the life of the program.	Retain documentation for the life of the program.
--	---	---

3) Safety Assurance Requirements

Requirement Citation	Requirement Description	Examples
FAA 1100.161 3.3a.1	Regularly scheduled internal ATO inspections of air traffic control, airway facility operations and maintenance, acquisition programs, and the ATO Aviation System Standards (AVN) organization.	Conduct and document regularly scheduled internal inspections of air traffic control, facility operations and maintenance. In addition, conduct and document regularly scheduled internal inspections of acquisition programs and AVN.
FAA 1100.161 3.3a.10	A process that periodically verifies that the controls required to mitigate hazards identified during risk assessments, and tracked in the hazard tracking and risk resolution system, are being met throughout the NAS. The ATO will develop and implement a methodology to determine the frequency of verification based on risk classification at a minimum.	
FAA 1100.161 3.3a.2	Internal ATO no-notice spot inspections of Air Traffic Control, and Airway Facility Operations and maintenance, including the ATO AVN organization, conducted by a party independent of the service organization that is inspected.	Conduct and document no notice, third party inspections of air traffic control, facility operations and maintenance.
FAA 1100.161 3.3a.4	Development of minimum NAS service level availability requirements, which includes validation and verification of these requirements for new systems entering the NAS and hardware, and/or software improvements to existing systems.	Demonstrate internal oversight, evaluation, and quality assurance through documentation and guidance material.
FAA 1100.161 3.3a.5	Monitoring and validation of NAS service availability standards, which include the comparison of fielded service availability performance within the standards.	Develop standards and guidance for NAS service availability. Provide measures for ATO NAS service availability against standards.
SMS 1.09	The ATO shall assess the effectiveness of the SMS in managing the safety of the NAS.	Continually assesses SMS effectiveness and document the process.
SMS 1.11	ATO shall track and share safety data (as defined in FAA Order 1100.161 Section 3.3.c) throughout the FAA.	Continuously track and share operational safety data (OE's, RI's, etc.). Provide evidence of tracking and sharing of hazard data. In addition, track and share SMS implementation data.

SMS 1.11	ATO shall track and share safety data (as defined in FAA Order 1100.161 Section 3.3.c) throughout the FAA.	Continuously track and share operational safety data (OE's, RI's, etc.). Provide evidence of tracking and sharing of hazard data. In addition, track and share SMS implementation data.
SMS 1.13	The ATO SMS shall include a mechanism for identifying the need for safety enhancing measures.	Identify the need for additional controls in the NAS through the application of SMS.
SMS 3.05	The ATO SMS shall provide continuous monitoring and regular assessment of the safety level achieved.	Constantly monitor, assess and document safety level achieved.
SMS 5.0	All activities undertaken in an Air Traffic System (ATS) safety management program shall be documented. All documentation shall be retained for the life of the program.	Document ATO Safety Assurance activities.
SMS 6.0	The ATO SMS shall establish a formal incident reporting system to facilitate the collection of data on actual incidents and potential safety hazards related to the provision of ATS.	
SMS 6.01	The ATO SMS shall collect data from the NAS on safety incidents.	Collect data from the NAS regarding safety incidents.
SMS 6.02	The ATO SMS shall monitor overall safety levels and detect any adverse trends.	Detail a process to detect trends in safety metrics.
SMS 7.0	Reports concerning the availability and reliability of ATO facilities and systems, such as failures and degradations of communications, surveillance and other safety significant systems and equipment shall be systematically documented, reviewed and investigated by the ATO in order to detect any hazards, including adverse trends.	Detail a process to ensure reports of failures and degradations of NAS systems are reviewed.
SMS 9.0	ATO shall conduct scheduled and unscheduled audits and evaluations of ATO service units that have the ability to change the NAS. ATO shall conduct formal reviews of the audit and evaluation results reported by service units.	
SMS 9.01	The ATO Safety Management System (SMS) shall provide for the conduct of safety reviews by all ATS units as part of the SMS continuous improvement process.	Conduct reviews of the SMS processes.
SMS 9.01.a	ATO shall publish an audit schedule quarterly.	Publish an audit schedule quarterly.

SMS 9.02	ATO shall conduct audits that cover, at a minimum, all items listed in ICAO doc 4444 paragraph 2.5.2.	Maintain a documentation system that ensures that manuals are complete, concise, and up-to-date. (ICAO doc 4444, 2.52a)
----------	---	---

4) Safety Promotion Requirements

Requirement Citation	Requirement Description	Examples
SMS 1.05	The ATO shall comply with established safety standards and the approved procedures and standards contained in the approved SMS.	The COO is lead of implementation of safety culture and COO ensures periodic status reporting for safety culture is being conducted.
SMS 1.10	All ATO executives, directors, managers, and practitioners shall be trained in SMS.	Identify ATO personnel who require SMS training and ensure training is received.
SMS 1.12	ATO shall share safety-related lessons learned throughout the FAA.	Publish safety lessons learned and ensure lessons learned are available to the entire FAA.
SMS 10.0	ATO shall document competency requirements, and where appropriate credentialing or certification requirements, for Safety Managers and Engineers, Air Traffic Controllers and Air Transportation System Specialists.	Document competency requirements for the safety managers and safety engineers.
SMS 11.0	Safety Managers and Engineers, Air Traffic Controllers and Air Transportation System Specialists shall meet the competency, credentialing, and certification requirements documented in the approved SMS Manual and/or contained in other related FAA orders, handbooks and guidance materials.	Ensure safety managers and engineers meet competency requirements.

6. OTHER CONSIDERATIONS

a. Clarification of Approval Criteria for the ATO SMS

FAA Order 1100.161 stipulates that ATO must “develop and maintain an SMS and submit it and any changes thereto, to AOV for approval.” Determination of compliance by ATO will be on the basis of the AOV V&V process. The validation part of the process ensures that the ATO SMS requirements are correct. Audits are conducted in the verification part of the process to ensure that facilities are in compliance with these requirements.

For example, a V&V audit reveals that a number of facilities are not in compliance with ATO SMS requirements. Would this, in itself, justify a non-approval determination for the SMS? Typically, the answer would be no. Approval would be granted unless all, or a very large number of facilities, were not in compliance. In this case there is the possibility of a system-wide problem that could, *in the absence of corrective action*, result in a determination of non-approval. Generally, approval requires that the following conditions be met:

Condition 1: The ATO Safety Management System (as defined in paragraph 4 of this SOC) fulfills the requirements enumerated in paragraph 6 of this SOC.

The SMS is defined as an “integrated collection of processes, procedures, policies, and programs that are used to...manage...safety risk.” Condition 1 requires that these processes, procedures, policies and programs completely, consistently, and unambiguously reflect all relevant FAA SMS requirements.

Condition 2: Absence of large-scale, systemic non-compliance with ATO SMS requirements.

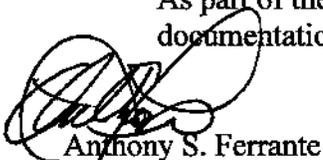
In a case of large-scale systemic non-compliance with ATO SMS requirements, the efficacy of corrective actions taken to mitigate that non-compliance would have to be evaluated before SMS approval could be granted. Evidence of non-systemic non-compliance, however, would not generally result in a determination of non-approval providing scheduled and unscheduled internal audits and evaluations have been planned to clearly reveal the non-compliance issues.

b. ATO SMS Validation and Verification Package

As described in this SOC, the validation and verification process is executed by AOV...

- (i) approving the ATO SMS manual and policies.
- (ii) reviewing and evaluating documents including Service Unit and facility Standard Operating Practices.
- (iii) receiving from ATO, prior to a formal request for approval of its SMS, a V&V package containing relevant orders, manuals, and SOPs from each of the affected Service Units.

As part of the audit planning process, AOV will request selected facilities to provide documentation relevant to the SMS V&V process.



Anthony S. Ferrante
Director, Air Traffic Safety Oversight Service

Attachment: Appendix

Appendix:

DEFINITIONS (SOC 08-07)

a. Acceptance

The process whereby the regulating organization has delegated the authority to the service provider to make changes within the confines of approved standards and only requires the service provider to notify the regulator of those changes within 30 days. Changes made by the service provider in accordance with their delegated authority can be made without prior approval by the regulator.

b. Approval

The formal act of approving a change submitted by a requesting organization. This action is required prior to the proposed change being implemented.

c. Assumptions

Characteristics or requirements of a system or system state that are neither validated nor verified.

d. ATO Safety Personnel

ATO personnel who perform direct safety-related air traffic control services, and/or certification on certifiable systems/subsystems/equipment or services in support of the NAS.

e. Cause(s)

Events that result in a hazard or failure. Causes can occur by themselves or in combinations.

f. Configuration Management

A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

g. Control

Anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls must be written in requirement language. There are three types of controls:

1) Validated

Those controls and requirements that are unambiguous, correct, complete, and verifiable.

2) Verified

Those controls and requirements that are objectively determined to have been met by the design solution.

3) Recommended

Those controls that have the potential to mitigate a hazard or risk but have not yet been validated as part of the system or its requirements.

h. Credentialing Program

A program for issuing, amending and removing credentials of ATO safety personnel, examiners and others, as appropriate, to ensure their currency and continued competency to perform safety functions as described in AOV's Credentialing order.

i. Effect

A description of the potential outcome or harm of the hazard if it occurs in the defined system state.

j. Hazard

Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.

k. Letter of Correction

Formally documents an ATO correction of an instance of non-compliance.

l. Letter of Investigation

Provides official notification to ATO that it has not been able to informally resolve an alleged non-compliance issue. The letter informs ATO of the specific matter being investigated and provides ATO an opportunity to respond in writing.

m. Maintenance

Any repair, adaptation, upgrade, or modification of NAS equipment or facility.

n. Oversight

To validate the development of a defined system and verify compliance to a predefined set of standards; Regulatory Supervision.

o. Requirement

An essential attribute or characteristic of a system. It is a condition or capability that must be met or passed by a system to satisfy a contract, standard, specification, or other formally imposed document or need.

p. Risk

The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. There are three types of risk: (1) initial, (2) current, and (3) residual.

1) Initial Risk

The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment.

2) Current Risk

The predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls may be used in the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

3) Residual Risk

The remaining risk that exists after all control techniques have been implemented or exhausted, and all controls have been verified. Only verified controls can be used for the assessment of residual risk.

q. Safety Council

A forum for top management officials from AOV and the ATO Safety to meet and discuss non-compliance and other safety issues in an attempt to resolve those issues.

r. Safety Directive (SD)

A mandate from AOV to ATO to take immediate corrective action to address a non-compliance issue that creates a significant unsafe condition.

s. Safety Management System (SMS)

An integrated collection of processes, procedures, and programs that ensure a formalized and proactive approach to system safety through risk management. Risk assessments are required for all changes to identify safety impacts. The SMS is a closed-loop system ensuring that all changes are documented and all problems or issues are tracked to conclusion.

t. Safety Requirement

A control written in requirements language.

u. System

An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services.

v. System Safety

The application of technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project, program, or activity.

w. System State

An expression of the various conditions, characterized by quantities or qualities, in which a system can exist.

x. Validation

The process of proving that the functions, procedures, controls, and safety standards are correct and the right system is being built (i.e., the requirements are unambiguous, correct, complete, and verifiable).

y. Verification

The process that ensures that the system requirements have been met by the design solution and the system is ready to be used in the operational environment for which it is intended.

z. Warning Notice

A notice that brings to ATO attention that immediate action is required to correct a significant unsafe condition. It warns that if the issue is not corrected, a Safety Directive (SD) mandating specified action will be issued. In emergency situations, where time does not permit the issuance of a warning notice, a SD may be issued without a warning notice.