



U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
Air Traffic Organization Policy

**ORDER
JO 6000.50C**

Effective Date:

04/15/2009

SUBJ: Technical Operations National Airspace System (NAS) Integrated Risk Management

- 1. Purpose.** This order establishes policies regarding Safety Risk Management (SRM) and Operational Risk Management (ORM) in the Technical Operations organization. Both SRM and ORM policy have been integrated into one document to assist field managers with risk management activities.
- 2. Audience.** This order is distributed in headquarters to group level within the Air Traffic Organization (ATO), to group level within the Technical Operations, En Route and Oceanic, Terminal and System Operations Service Areas; and to all Technical Operations, En Route and Oceanic, and Terminal field offices with a standard distribution.
- 3. Where Can I Find This Order.** You can find this order on the Directives Management System (DMS) website: https://employees.faa.gov/tools_resources/orders_notices/.
- 4. Cancellation.** Order 6000.50B, Airway Facilities National Airspace System Operations Procedures, dated June 29, 2001, is cancelled.
- 5. Explanation of Policy Changes.** This order has been changed to incorporate SRM policy and introduce the strategy for ORM. The order has been completely re-created with limited content included from the previous version. One policy that remains virtually the same regards Standard Operating Procedures (SOPs). SOP 300-SOP describes the procedures that govern the creation, revision, implementation and cancellation of SOPs. The SOP 300-SOP is available on https://intranet.faa.gov/faaemployees/org/linebusiness/ato/operations/technical_operations/ajw163/sop/. The SOPs must not deviate from or supersede directives.
- 6. Implementation.** While it is encouraged that organizations begin including Generic Site Implementation Plans (GSIPs) and Local Site Implementation Plans (LSIPs) with their implementation activities after the effective date of this order, those plans will become mandatory for all implementation activities described in this order that have a construction or installation start date after July 15, 2009. The use of the Integrated Risk Management Checklist (IRMC) is mandatory upon the effective date of this order. If a GSIP and/or LSIP has not been prepared for an implementation activity that has a construction or installation start date prior to July 26, 2009, and that activity requires an IRMC in accordance with this order, then the IRMC questions regarding GSIPs and LSIPs should be answered as "No" and the term "N/A" should be stated in the comments field.
- 7. Background.** There have been many versions of Risk Management policy and guidance provided to the workforce over the past several years. Throughout these iterations, the term "Risk Management" focused primarily on "Operational" risk management. In particular, the first version of this order provided extensive guidance and a detailed checklist on what must be accomplished before an activity

could be started, with the intent of minimizing interruptions to the NAS. The second version was significantly streamlined and addressed risk management from a philosophical standpoint and again, every use of the term “Risk Management” primarily meant “Operational” risk management. The ICAO Annex 11 document dated November 1, 2001 required all member states to establish a Safety Management System (SMS). On March 19, 2007 the FAA ATO published Order JO 1000.37, Air Traffic Organization Safety Management System, which establishes SMS policy for the ATO. The establishment of this policy introduced the concept of SRM. This order integrates both ORM and SRM into one policy document to help clarify both processes and provide guidance to field managers to ensure risk management is being implemented appropriately.

8. Authority to Supplement. This order may be supplemented to add further detail to the identified processes; however, supplements may not subtract from the policy described herein. All supplements must be approved by the office of primary responsibility for this order.

9. Definitions.

a. Safety Risk Management (SRM) - A formalized, proactive approach to system safety. SRM is a methodology applied to all NAS changes to ensure hazards are identified and unacceptable risk is mitigated prior to the change being made. It provides the framework to ensure that once a change is made, it continues to be tracked throughout its lifecycle.

(1) SRM is a fundamental component of the SMS. It is a systematic, explicit, and comprehensive approach for managing safety risk at all levels and throughout the entire scope of an operation and lifecycle of a system. It requires the disciplined assessment and management of safety risk.

(2) The goal of SRM is to ensure that safety-related changes are documented; risk is assessed and analyzed; unacceptable risk is mitigated; hazards are identified and tracked to resolution; the effectiveness of the risk mitigation strategies is assessed; and the performance of the change is monitored throughout its lifecycle. All safety risk assessments must be documented in either a Safety Risk Management Document (SRMD) or a Safety Risk Management Decision Memorandum (SRMDM). SRMDs are required when risks have been identified and must be accepted. SRMDMs are required when no credible risks have been identified. See Appendix 2 for the roles and responsibilities within Technical Operations when completing SRM assessments.

b. Operational Risk Management (ORM) - The process of assessing an activity for its potential to negatively impact the NAS from an operational perspective. This impact could be in the form of causing flight delays, excessive financial costs, project schedule delays, political implications, Occupational Safety and Health type impacts, negative effects on performance metrics, etc. Whenever SRM and ORM conflict, SRM must always take precedence, e.g., bypassing the local shutdown capability to keep a system on the air, designing a modification to be installed on a hot system because a shutdown cannot be taken, etc., mitigate operational risks but introduce potentially unacceptable safety risks.

c. Generic Site Implementation Plan (GSIP) – A plan written by the implementing organization (typically a program office) that describes the steps necessary to implement a system or

equipment into the NAS. These plans are intended to cover all aspects of an installation that are common to a system or equipment regardless of where it is being installed into the NAS.

d. Local Site Implementation Plan (LSIP) – A plan that describes the local requirements to implement a system or equipment into the NAS. Typically the LSIP only identifies the items that are different from the GSIP due to local conditions.

e. Integrated Risk Management Checklist (IRMC) – An automated tool required to be completed prior to allowing certain activities to move forward. These are implementation, modification and certain periodic maintenance activities that could have a negative impact on the NAS. See Appendix 1 for an example of the checklist.

f. Standard Operation Procedures (SOPs) – SOPs are the method for documenting procedures within Technical Operations. Procedures can be published as an SOP making them more flexible to change.

g. System Safety Assessment Report (SSAR) – During the acquisition process, a report to provide management an overall assessment of the safety risk associated with the system prior to fielding, but also must be employed, prior to operation of the system. This is accomplished by providing summaries of the analyses and testing results. The report contains an overall assessment of the program from the analyses performed and a status of all existing and recommended safety requirements. The SSAR identifies all safety features of the system, design and procedural hazards that may be present in the system being acquired, and specific procedural controls and precautions that should be followed.

10. Safety Risk Management Requirements. SRM is required whenever there is a proposed change to the NAS. The initiators of these changes are generally program offices, 2nd Level Engineering and Engineering Services. However, local System Support Centers (SSCs) can also initiate changes to the NAS requiring SRM assessments. Appendix 2 is the policy for how SRM will be accomplished within Technical Operations. The following actions always require SRM assessments to be completed:

a. Any activity baselined under Configuration Management (requiring a Configuration Control Decision).

b. All implementation activities. See paragraph 11 for these SRM requirements.

c. All System Support Directives (SSDs). SRM is completed by the authoring organization with authority to implement the SSD (typically 2nd Level Engineering). Local SRM is only required if the SSD is initiated locally or there is a deviation from the installation instructions.

d. Required routine maintenance. SRM is required on the maintenance directive including schedules, tasks and tolerances. Local SRM is not required unless a routine maintenance activity is initiated locally or there is a deviation from the maintenance instructions.

e. Any new requirement given to 2nd Level Engineering organizations to implement. The requirement itself must have an SRM assessment completed before 2nd Level Engineering can accept

the requirement and begin developing a solution.

11. Operational Risk Management Requirements. ORM must be performed on any activity having the potential to negatively impact the NAS from an operational perspective. To assist in performing ORM, an IRMC has been developed (see paragraph 13 for a detailed description of the IRMC). The items in the checklist should be taken into account prior to performing any activity with the potential to negatively impact the NAS from an operational perspective. The following activities require ORM to be formally documented and therefore an IRMC must be completed before the activity can proceed:

- a. All implementation activities that interface with or have the potential to impact the operational NAS.
- b. All implementation activities in an operational Air Traffic facility (Air Traffic Control Tower, Terminal Radar Approach Control, Air Route Traffic Control Center [ARTCC], Combined Center Radar Approach Control) except non-intrusive site surveys and staging activities.
- c. All implementation activities (including site surveys and staging activities) on an operational airport.
- d. For services with a response code of 4 hours or sooner: all modifications requiring a full service interruption and all modifications requiring physical actions on an operational NAS system (in use or available for use).
- e. Certain maintenance activities will require an IRMC to be completed before performing the maintenance. These are generally maintenance activities requiring outages on critical facilities at high impact locations, e.g., rotating the Power Conditioning System busses at an ARTCC, changing the antenna oil on the ASR at a high impact airport, etc. Other maintenance activities pose so little operational risk to the NAS that they will not require a checklist to be completed, e.g., maintenance on facilities at low activity airports, non-intrusive maintenance tasks, etc. Local Technical Operations and Air Traffic management will meet annually and determine which maintenance activities will require a checklist to be completed prior to performing that activity. This list will be developed prior to the start of the calendar year and will be published and provided to the control centers.

Note: SRM and ORM may be required on the same activity (and frequently are) but have different objectives. See Appendix 4 for a chart summarizing these requirements.

12. Site Implementation Plan Requirements.

a. Site Implementation plans are required for every implementation activity. Program Offices must develop GSIPs for nationally deployed activities and these plans may require local adaptation for each site affected by the activity. GSIPs and the SRM assessment of those GSIPs must be completed prior to installation of the first system (key site is considered the first system; therefore a GSIP is required prior to key site installation). At a minimum, every GSIP must include the following:

- (1) A thorough description of the scope of the project.

(2) A clear identification of all activities requiring an IRMC.

(3) A clear identification of all items requiring local adaptation due to unique site requirements or configurations. Any such items affecting safety must be clearly identified and requirements to conduct SRM assessments locally on these items must be included.

(4) Any mitigations and assumptions regarding local facility operations (specific equipment availability, personnel credentials, personnel availability, tasks required by local Technical Operations personnel etc.). Deviations from the required mitigations or assumptions require local SRM.

(5) An SRM section that identifies all hazards, mitigations and residual risks identified in the System Safety Assessment Report (SSAR). If an SSAR was not completed, then the hazards, mitigations and residual risks identified prior to the In-Service Decision must be included in this section.

(6) An SRMD or SRMDM as the result of completing a safety assessment on the Site Implementation Plan.

(7) LSIPs are frequently required to add detail to the GSIP and LSIPs are required for all local projects. In addition to the applicable items above, these LSIPs must include a detailed coordination process that includes all organizations that require coordination prior to moving forward with the activity. Additionally, all LSIPs require SRM.

b. SRM assessments must be completed on all Site Implementation plans. If risk mitigations are dependent on any activity by the local Technical Operations or Air Traffic managers, this activity must be clearly communicated to the local Technical Operations/Air Traffic managers.

13. Roles and Responsibilities.

a. Implementer/Change Agent. This can be a national program office, Engineering Services, Technical Support Operations Group and/or potentially the local SSC (although rarely). These organizations are responsible for developing the site implementation plan, completing the SRM assessment on the plan, and initiating the IRMC (with significant input from the local SSC and Air Traffic).

b. Local Technical Operations Manager. This is usually the SSC manager being affected by the activity. This can also be a group level or district manager depending on the situation. This individual is responsible for working with the local Air Traffic manager, as necessary, during the risk management process and to implement all mitigations assigned to the local SSC as part of the SRM on the Site Implementation Plans.

c. Local Air Traffic Manager. This is normally the Terminal or En Route manager of the facility being affected by the activity. When activities are being performed at an unstaffed location, the manager of the Air Traffic facility controlling the airspace will serve as the local Air Traffic manager. This individual is responsible for working with the local Technical Operations manager as necessary during the risk management process.

d. Technical Operations District Manager. This is the manager (or designee) of the Technical Operations district where the activity is taking place. This individual is responsible for ensuring the IRMC is completed to his/her satisfaction. This individual has the final approval to allow an activity to proceed and in making that decision, must ensure all items on the IRMC are complete or a valid justification is documented for excluding an item from being complete.

e. Air Traffic District Manager. This is the manager (or designee) of the Terminal or En Route district where the activity is taking place. This individual is responsible for jointly approving the IRMC with the Technical Operations district manager. This individual has the authority to stop an activity from moving forward but only the Technical Operations district manager has final authority for allowing an activity to move forward.

f. Control Centers. This can be a Service Operations Center (SOC) or Operations Control Center (OCC) depending on the scope of the project. The control center is responsible for coordinating the activity with the impacted Service Units and ensuring appropriate Notices to Airmen (NOTAMs) are issued or cancelled. They will also assist with any contingency planning and will remain aware of the activity and its status to ensure the impact on the overall NAS is minimized.

14. Integrated Risk Management Checklist (IRMC).

a. The IRMC is an automated tool that can be found on the FAA's Technet intranet site and must be completed for the activities described in paragraph 10 above. The checklist is both a gatekeeper to ensure no identified activity takes place without a checklist being completed and also serves as a memory jogger to ensure the appropriate risk management steps are being taken for the proposed activity.

b. Each checklist must be approved by the Technical Operations and Air Traffic district managers (or designee).

c. Every checklist will be available to be viewed nationally.

d. The initiator of the activity is responsible for initiating the checklist and determining who can input data into the checklist, who can modify the data in the checklist and who will be approving the checklist. Typically the initiator is the project engineer for implementation activities and the SSC manager or SOC for modification/maintenance activities.

e. The automated system will have an audit trail to easily identify who made changes to the data in a checklist.

f. When a checklist is approved, it will be automatically transmitted via e-mail to the appropriate control center (OCC, SOC), the initiator of the activity and any others that the local Technical Operations manager deems necessary.

g. The required checklist items are identified in the automated tool; however, examples of those items are briefly described below:

(1) Facility. This is the name of the facility as identified in the Facilities, Services and Equipment Profile (FSEP).

(2) Ident. This is the identifier of the facility as listed in the FSEP.

(3) Activity Title. The title of the project, modification, or maintenance activity.

(4) Activity description. This is a short statement (usually no more than one or two sentences) describing the activity and the facilities being affected. The identified facilities must match an FSEP facility.

(5) Proposed Start Date. The date the activity is scheduled to begin.

(6) Proposed Duration. The estimated duration of the activity.

(7) Have we briefed appropriate stakeholders (Air Traffic, Airports, Technical Operations, Control Center, etc.)? Depending on the activity, a formal briefing may be required. At a minimum, the local Air Traffic manager and the appropriate control center must be briefed on the activity. This briefing must include the items in the site implementation plan and any contingencies planned. The names and titles of the individuals briefed must be captured under this item in the checklist.

(8) Is the activity scheduled during a time of minimal impact (Weather, VIP Traffic, Holidays, Air Traffic Operational Activity Level, etc.)? When scheduling the activity, ensure it will have the least impact to the NAS. Depending on the scope and type of activity, take into account the forecasted weather conditions; whether or not there are planned VIP movements in the airspace affected by the activity; whether or not the activity is scheduled during a high travel period; and what the Air Traffic operations activities are. The goal is for the proposed activity to have no impact on the NAS operations even if unforeseen circumstances should arise.

(9) Has SRM been completed on the Site Implementation Plan? All site implementation plans must have an SRM assessment completed resulting in either an SRMD or SRMDM. These documents should be reviewed prior to completing this portion of the checklist.

(10) Are all SRM mitigations dependent on local actions clearly understood by local management? When an SRM assessment is completed on the Site Implementation Plan, any mitigations dependent on actions by the local facility, must be clearly communicated to the local manager. The local manager must understand the mitigations and his/her responsibilities in carrying out the identified actions.

(11) Has local technical oversight been established? Depending on the scope and type of activity, the local SSC must designate someone to oversee the activity. This individual should have the appropriate skills to ensure the activity is being completed in accordance with the site implementation plan and all safeguards to minimize impact to the NAS.

(12) Have requirements of the Strategic Shutdown Committee been met? Depending on the type and duration, the Strategic Shutdown Committee must approve the outage associated with the activity. If the Strategic Shutdown Committee is not required to approve the outage, the rationale should be documented in this section. See FAA Order 6000.15, General Maintenance Handbook for National Airspace System (NAS) Facilities, for the requirements of the Strategic Shutdown Committee.

(13) Has the appropriate control center been coordinated with? The activity must be coordinated with the responsible OCC/SOCs. The control center must use this information to monitor the activity as it progresses to minimize the impact to the NAS.

(14) Are there any potential affects to air quality, fire alarms, etc., at Air Traffic Control Facilities? When developing the site implementation plan and contingency planning, the impact this activity may have on air quality and fire alarms must be considered. These include creating fumes, releasing mold, disturbing asbestos, creating smoke, etc. If the answer to this question is yes, the actions being taken to mitigate the effect must be documented in this section.

(15) Have worst credible human errors been planned for and mitigated? During the contingency planning process for this activity, the credible human errors must be considered and planned for. The goal is to have no impact on the NAS when even the worst credible human error is committed.

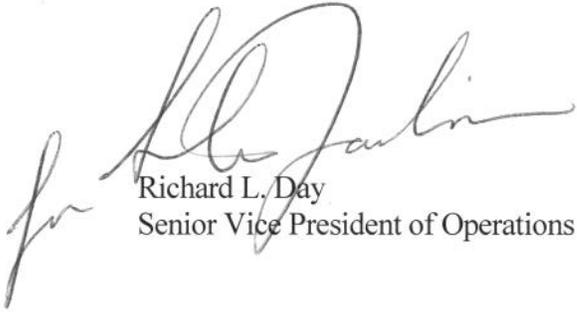
(16) Are specific resources required for this activity, e.g., Technical Operations/Air Traffic staffing, backup power, standby equipment, alternate procedures, etc? During the contingency planning process, all potential scenarios should be taken into account and the appropriate mitigations to those scenarios must be prepared. This can involve having extra Air Traffic and/or Technical Operations personnel with the proper skills standing by. This could also involve having portable engine generators, air conditioners, heaters, etc., standing by. The goal is to ensure the various scenarios taken into account will have no impact on the NAS if they should develop.

(17) If the activity requires operation on an airport movement area, has the appropriate manager briefed all parties on required procedures for contacting Air Traffic, the airport layout and directions on how to get to the facility, and minimizing operations within the airport movement area? Operations on an airport movement area require all parties to be thoroughly briefed on the proper procedures for operating within the movement area. This includes ensuring personnel have the proper training, communications equipment, know the phraseology and procedures. The goal is to ensure that no runway incursions are committed during this activity.

(18) Has the proper NOTAM been issued and confirmed that it accurately reflects the activity being planned? Depending on the activity, a NOTAM may be required prior to starting the activity. The issuance of the NOTAM must be confirmed when the activity is started. When the activity is completed, it must be confirmed that the NOTAM was cancelled. If the activity does not require a NOTAM to be issued, this must be documented in this section.

(19) Activity is Approved. The district manager (or designee) for Technical Operations and Air Traffic must both approve the activity on the checklist prior to moving forward. When signing this checklist, the managers are stating all items on the checklist have either been completed or justified as to why they were not completed to the satisfaction of the managers.

h. The IRMC will have the same retention period as the facility maintenance logs.

A handwritten signature in cursive script, appearing to read "for R. L. Day".

Richard L. Day
Senior Vice President of Operations

Appendix 1. NAS Integrated Risk Management Checklist

1. Facility:		2. Ident:	
3. Activity Title:			
4. Activity Description:			
5. Proposed Start Date:		6. Proposed Duration:	
7. Have the appropriate Stakeholders been briefed (Air Traffic, Airports, Technical Operations, Control Center, etc.)?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
8. Scheduled during time of minimal impact (Weather, VIP, Traffic, Holidays, Aircraft Activity Level, etc.)?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
9. Has an SRM assessment been completed on the site implementation plan?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
10. Are all SRM mitigations dependent on local actions clearly understood by local management?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
11. Has local technical oversight been established?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
12. Have requirements of the Strategic Shutdown Committee been met?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			
13. Has the appropriate Control Center been coordinated with?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>			

Appendix 1. NAS Integrated Risk Management Checklist, continued

14. Are there any affects to air quality, fire alarms etc., at Air Traffic Control facilities?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If Yes, Explain:</i>		
15. Have Worst credible human errors been planned for and mitigated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>		
16. Are specific resources required for this activity, e.g., Technical Operations/Air Traffic Staffing, backup power, standby equipment, alternate procedures etc?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>		
17. If the activity requires operation on an airport movement area, has the appropriate manager briefed all parties on: required procedures for contacting Air Traffic, the airport layout and directions on how to get to the facility and minimizing operations within the airport movement area?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>		
18. Has the proper NOTAM been issued and confirmed it accurately reflects the activity being planned?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<i>If No, Explain:</i>		
19. Activity is approved:		
_____ Technical Operations District Manager Date: (or designee)	_____ Applicable Terminal or En Route District Manager (or designee)	_____ Date:

Appendix 2. Safety Risk Management Process

1. One of the key components of a successful Safety Management System (SMS) is the Safety Risk Management (SRM) process. The Director of Safety and Operations Support, and within that organization the Manager of the Safety and Quality Assurance Group, has overall responsibility for the effective implementation of SRM within Technical Operations. It is critical that all organizations have a clear understanding of the SRM requirements, accountabilities, and authorities for Technical Operations SRM products. SRM products consist of both SRM Documents (SRMD) and SRM Decision Memoranda (SRMDM).

Effective immediately, the following applies to the SRM documentation in Technical Operations:

a. The organization initiating a change to the National Airspace System (NAS) is responsible for the safety assessment of the proposed change and documenting that change in an SRMD or SRMDM in accordance with Technical Operations and ATO-wide SMS policy.

b. **SAFETY REVIEWER.** Previously, the Manager of the Safety Management and Quality Assurance Group reviewed all SRM products for quality and compliance with policy. With the recent establishment of reviewers in each Directorate, these reviewers now serve this quality control function for the Safety Management and Quality Assurance Group. Specifically, these reviewers are nominated by each Director and approved by the Manager of the Safety Management and Quality Assurance group and are expected to review and provide a quality control check for SRMDs and SRMDMs. For SRMDs, this review focuses primarily on the adequacy of the document in providing the necessary staff work to the Risk Acceptor. For SRMDMs, the review focuses on the adequacy of the rationale as to why the change does not impact the safety of the NAS. The reviewer is not expected to have a detailed understanding of the NAS system or all possible causes of hazards; however, a functional understanding of the NAS and its potential effects on safety is essential to provide effective quality control of the SRMD or SRMDM. The reviewer will sign any SRMD or SRMDM as the "Technical Operations Safety Reviewer" and the Manager of the Safety Management and Quality Assurance Group will provide initial familiarization with the requirements for these reviewers and follow-up feedback and recurring familiarization as needed.

c. **APPROVER.** SRMDs require an approver signature. This individual is the management official responsible and accountable for the overall process used and the accuracy of the SRMD. Except for those situations defined in ATO-wide SMS policy requiring a different signature level; the Technical Operations approver is the group manager (or equivalent K- band manager) of the initiator of the change.

d. **RISK ACCEPTOR.** Except for those situations defined in ATO-wide SMS policy as requiring a different signature level, in Technical Operations the Risk Acceptor of an SRMD is the Director of the organization initiating the change. SRMDs are kept and maintained by the organization responsible for the change for the life of the system or change.

e. **SRMDM SIGNER.** SRMDMs are signed by the management official responsible and accountable for the overall SRMDM and its assertion there are no credible hazards from the change. In Technical Operations, at a minimum, this is the group manager (or equivalent K- band manager) of

Appendix 2. Safety Risk Management Process, continued

the initiator of the change. This individual signs as the author of the memorandum and it is kept on file for the life of the system or change.

2. The Safety Management and Quality Assurance Group will continue to periodically review safety documentation for Quality Assurance purposes; therefore, a copy of all finalized SRMDs and SRMDMs must be sent electronically to the Manager of the Safety Management and Quality Assurance Group, AJW-18.

Additionally, each Directorate will formally document their internal SRM practices, with submittal to the Manager of the Safety Management and Quality Assurance Group, AJW-18 for review and concurrence. Any future changes to the Directorate's documented internal SRM practices must also be forwarded to the Manager of the Safety Management and Quality Assurance Group, AJW-18 for review and concurrence.

Appendix 3. List of Acronyms

ARTCC – Air Route Traffic Control Center
ASR – Airport Surveillance Radar
ATCT – Airport Traffic Control Tower
ATO – Air Traffic Organization
CERAP – Combined Center Radar Approach Control
FSEP – Facilities, Services, Equipment Profile
GSIP – Generic Site Implementation Plan
ICAO – International Civil Aviation Organization
ISD – In-Service Decision
IRMC – Integrated Risk Management Checklist
LSIP – Local Site Implementation Plan
NAS – National Airspace System
NOTAM – Notice to Airmen
OCC – Operations Control Center
ORM – Operational Risk Management
OSHA – Occupational Safety and Health Administration
PCS – Power Conditioning System
PM – Periodic Maintenance
SMS – Safety Management System
SOC – Service Operations Center
SOP – Standard Operating Procedure
SRM – Safety Risk Management
SRMD – Safety Risk Management Document
SRMDM – Safety Risk Management Decision Memorandum
SSAR – System Safety Assessment Report
SSC – System Support Center
SSD – System Support Directive
TRACON – Terminal Radar Approach Control
TSOG – Technical Services Operations Group

Appendix 4. Summary of SRM and ORM Requirements

	SRM	IRMC¹
Implementation Activities	<p>Program Office (or other project owner) builds a Generic SIP, assesses & accepts Safety Risk prior to installation of the first system. Any locally required decisions/mitigations and safety issues must be clearly defined in the GSIP.</p> <p>Facility implementation designer/ implementer - Reviews the GSIP. Assesses and accepts the Safety Risk of local decisions and any deviations from the GSIP.</p>	<p>On airport – IRMC is required.</p> <p>Off airport, but involving or co-located with operational NAS – IRMC is required, <u>except</u> for non-intrusive staging or site survey activities.</p> <p>Off airport and not involving or co-located with operational NAS – IRMC is not required.</p>
Modifications	<p>Mod issuer (typically Second Level Engineering) completes SRM on mod (including the Safety Risk of installation instructions).</p> <p>Facility mod implementer– No local SRM required, unless mod instructions are not followed or mod is locally developed.</p>	<p>IRMC is required for modifications to equipment with a restoration response code of 4 hours or sooner if</p> <ol style="list-style-type: none"> (1) work requires a full service interruption, or (2) work is performed on operational equipment (in use or available for use). <p>Note: IRMC is not required for modification to Standby/Backup equipment when such equipment is released from service by all users or is advertised to all users as unavailable.</p>
Required Maintenance	<p>Author of Maintenance Directive completes SRM.</p> <p>Facility maintainers – No SRM required unless there are deviations from requirements of maintenance directive or maintenance actions are defined at Service Area, District, or facility level.</p>	<p>IRMC is required only for those maintenance actions defined locally as having significant operational risk. Examples may include work on critical power bus or other potential single points of failure at high impact facilities.</p>

¹ The applicable actions identified on the IRMC should typically be considered before any maintenance action. The IRMC column identifies activities where the formal documentation via the IRMC is required.