U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

ORDER 8040.4A

Effective Date
04/30/12

SUBJ: Safety Risk Management Policy

This order supports FAA Order 8000.369, *Safety Management System Guidance* and establishes requirements for how to conduct Safety Risk Management (SRM) in the FAA. It formalizes the use and communication of SRM across the FAA and describes the specific steps when performing SRM. This document does not define implementation schedules. Compliance with this order will be achieved in accordance with the FAA and Line of Business Safety Management System (SMS) implementation plans.

The FAA's mission is *"To provide the safest, most efficient aerospace system in the world."* To support its mission, the FAA is implementing an SMS that integrates the management of safety risk into business planning, operations, and decision making. This will enhance the safety of the flying public and strengthen the FAA's worldwide leadership in aviation safety.

The SMS consists of four components: Safety Policy, Safety Risk Management, Safety Assurance, and Safety Promotion. The objective of the SRM component is to provide supporting information for decision-makers by identifying hazards, analyzing safety risk, assessing safety risk, and developing controls. SRM facilitates streamlined communication and coordination across FAA organizations for enhanced safety risk decision making. All four components work together to enable the FAA to manage safety within the aerospace system.

Michael P. Huerta
Acting Administrator

Table of Contents

Chapter 1. General Information

1. Purpose of This Order. This order establishes the Safety Risk Management (SRM) policy for the FAA. It also establishes common terms and processes used to analyze, assess, and accept safety risk. The design of this policy is to prescribe common SRM language and communication standards to be applied throughout the FAA. Furthermore, the policy recognizes that FAA organizations have unique missions and requirements, so it allows flexibility in the application of SRM. Appendix A – *Definitions* contains definitions for terms used in this policy. Appendix B – *Acronyms* contains acronyms used in this policy.

2. Audience. FAA personnel in all FAA Lines of Business (Airports Organization (ARP), Commercial Space Transportation Organization (AST), Air Traffic Organization (ATO), and Aviation Safety Organization (AVS)) and the NextGen Organization (ANG).

3. Where Can I Find This Order. You can find this Order on the MyFAA Employee Web site: https://employees.faa.gov/tools_resources/orders_notices/. This Order is available to the public at http://www.faa.gov/regulations_policies/orders_notices/.

4. Cancellation. This order replaces FAA Order 8040.4, *Safety Risk Management*, dated June 26, 1998.

5. Background.

a. The FAA's mission is *"To provide the safest, most efficient aerospace system in the world."* To support its mission, the FAA is using a Safety Management System (SMS) to integrate the management of safety risk into business planning, operations, and decision making in order to enhance the safety of the flying public and strengthen the FAA's worldwide leadership in aviation safety. The SMS consists of four components: Safety Policy, Safety Risk Management, Safety Assurance, and Safety Promotion. These components work together to enable the FAA to manage safety within the aerospace system.

b. This document establishes the SRM policy for the FAA. This SRM policy will support the FAA's implementation of SMS by providing the ability to consistently conduct SRM. Further, along with Safety Assurance functions, SRM will assist the FAA in ensuring that hazards are identified and safety is managed to acceptable risk levels throughout the aerospace system.

c. The International Civil Aviation Organization (ICAO) has established frameworks for a State Safety Program (SSP) in member states and SMSs in product/service provider organizations. Because the FAA contains regulatory as well as product/service provider organizations, the FAA is implementing an SMS which will meet the tenets of both the SSP and SMS ICAO frameworks.

(1) **FAA as Product/Service Provider.** When an FAA organization is performing in the capacity as a product/service provider, such as the ATO, it is responsible for primary SRM because it has the ability to directly control safety risk associated with hazards identified in its operations. Specifically, the ATO owns the personnel, processes, equipment, and systems that comprise the National Airspace System (NAS). Therefore, the ATO, as a product/service provider, has control over the NAS operations and many of the hazards that exist in the operational environment. The ATO can, if necessary, even cease operations in certain environments, discontinue use of some systems,

alter the configurations or operating practices of their systems, etc. Further, ATO Management is directly responsible for NAS operations. Thus, ATO Management can accept and manage safety risk in NAS operations. Under certain circumstances, such as Federal financial participation in airport development projects, the FAA will coordinate SRM activities with airports to ensure that both parties' SRM responsibilities are completed in a complementary manner.

(2) **FAA as Regulator.** Regulators, such as AVS, AST, and ARP, work a level removed from actual operations. Within the limits of the regulator's authority, they can apply constraints to product/service provider activities and operations. These constraints can be thought of as secondary controls since they are not directly managing safety risk in operations. These secondary controls are promulgated by the FAA through regulations, standards, policy, guidelines, etc. The actual implementation of the controls rests with the product/service provider. Hazards with significant associated safety risk may exist, but because of the constraints within which the regulator must operate, the regulator may not be able to establish controls. Such constraints include: the regulator's legal authority (which is established by statute), technological limitations, or cost-benefit requirements for regulations. Thus, regulators may be forced to accept safety risk by default. When this is the case, the regulator must document the analysis and decision, apply the controls that it is able to, and establish a methodology to monitor the risk. At no point is the FAA, in an oversight capacity, responsible for performing SRM for an individual or organizational aviation product/service provider.

6. Scope.

a. This order supports FAA Order 8000.369, *Safety Management System Guidance* and describes the process used to conduct SRM in the FAA. Specifically, it formalizes the use of SRM across the FAA, is focused on safety in the aerospace system, describes the specific steps when performing SRM, and enables communication and coordination across FAA organizations for enhanced safety risk decision making.

b. This order is applicable to all FAA organizations, especially in terms of hazard identification and tracking, and safety risk control. It is expected that any hazards that cross organizations will be fully coordinated between organizations. Organizations should supplement this order with organizational process and procedure instructions to aid in promoting effective SRM and must collaborate with their respective and affected organizations when performing SRM.

Chapter 2. Safety Risk Management Process

1. General Information.

a. Introduction. SRM is one of the four components of the SMS that enable the FAA to manage safety within the aerospace system. SRM is composed of describing the system, identifying the hazards, and analyzing, assessing, and controlling safety risk.

b. Objective. The objective of SRM is to provide supporting information for decision-makers by identifying hazards, analyzing safety risk, assessing safety risk, and developing controls to reduce risk to an acceptable level. SRM facilitates communication and coordination across FAA organizations for enhanced safety risk decision making.

c. Applicability. This order applies to all FAA Lines of Business (ARP, AST, ATO, AVS) and ANG. Each of these organizations must (1) document when SRM must be applied within its organization, (2) engage other FAA organizations early and throughout their own SRM initiatives as appropriate, and (3) participate in SRM initiated by other FAA organizations as requested. In general, SRM is applied when making planned changes to the aerospace system and when potential and previously unidentified hazards and ineffective controls are discovered. SRM is used to evaluate the need for, and to develop, safety risk controls in the aerospace system. Effective SRM requires early and ongoing involvement by appropriate stakeholders.

d. Relationship Between SRM and Safety Assurance. While the focus of this policy is SRM, it is important to understand how SRM and Safety Assurance work together. The SRM process provides a system analysis, the identification of hazards, and the analysis and assessment of safety risk. As a result, safety risk controls are developed and, once they are determined to be practicable in reducing safety risk to an acceptable level, these controls are employed operationally. Safety Assurance is used to ensure that safety risk control strategies are in place, assess whether they are achieving their intended safety risk reduction objectives, and monitor for unintended consequences. If the controls are not adequately reducing safety risk, they are modified and/or additional safety risk controls are developed through SRM. This is one way SRM and Safety Assurance are integrated. Another way these functions work together is through the identification of potential new hazards or ineffective controls through Safety Assurance measures, which are then analyzed and assessed using SRM. Figure 2-1 depicts the SRM and Safety Assurance processes and their relationship to one another. This flowchart is representational. It shows the most obvious and frequent interactions between the SMS tenets of Safety Assurance and SRM. The two are closely intertwined at every step. There are three basic findings in the system assessment within Safety Assurance: (1) In conformance with requirements, (2) Not in conformance with requirements, or (3) Identification of a new hazard or ineffective control. When a new hazard or ineffective control is identified, the SRM process is used to further investigate. When a non-conformance to requirements is found, correction or corrective action is typically taken.

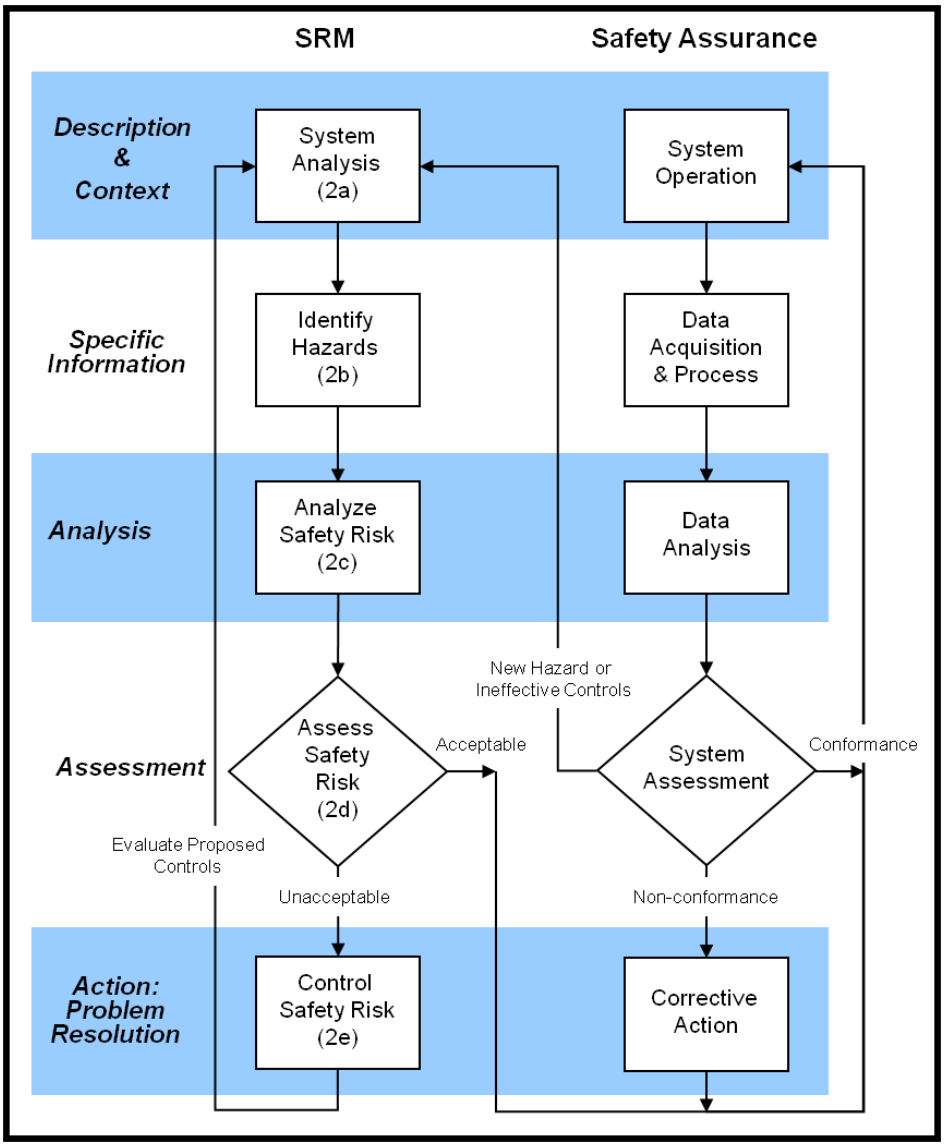

Figure 2-1: SRM and Safety Assurance Processes

e. SRM in the Operational Environment.

(1) Just as SRM is an integral part of the design and deployment of equipment and procedures, it is equally important to evaluating safety in the operational environment. There are additional considerations for SRM in the operational environment. Operational data provides quantitative information for evaluating failure modes, frequencies, and consequences. As such, it supports safety risk estimation by providing real world information.

(2) Sometimes, previously unidentified hazards are discovered or known hazards are found to have more safety risk than was initially predicted. Assessments may uncover safety risk that would have been unacceptable when the product or system was first put into service. This introduces a quandary, especially if controls to the newly-identified hazard require changes that cannot be instantly implemented. For this reason, SRM in the operational environment often necessitates short-term

acceptance of safety risk that is higher than would have been initially accepted while controls are being developed and implemented to lower the safety risk. For example, Aircraft Certification (AIR) has acceptable safety risk guidelines for continued short-term operation, as well as safety risk guidelines for acceptable long-term operation that may be different from initial certification. In this context, short term does not refer to a specific time period (for example, '90 days' or '1 year'), but rather refers to the period of time during which the safety risk of the hazard does not exceed the guidelines for continued operation.

(3) Additionally, safety risk controls are often subject to economic evaluation, which introduces further constraints on the mitigations that are implemented. Nonetheless, the general policies and concepts of this order apply to SRM in the operational environment.

f. SRM Teams.

(1) Depending on the issue under consideration, the safety risk analysis may be conducted by an individual or team within a single organization. Other times, a cross-organizational team of stakeholders must be formed to adequately address the scope and complexity of the issue. In order to be most useful to the decision-maker, SRM is best conducted by an individual who has, or a team whose members have, a diverse set of skills. Multiple disciplines should be represented on these teams, including those with expertise in operational, technical, engineering, and safety areas. Teams must include representatives from the various organizations that could be affected by the decision, which often means that multiple Lines of Business must be represented.

(2) Peer review is encouraged to strengthen decision-maker confidence in the fidelity of the SRM outputs. These peer reviews should be performed by different individuals than those who have conducted SRM, but with similar expertise as those on the SRM team.

g. Coordination Among Lines of Business. A hazard, its associated safety risk, and/or safety risk control(s) may impact multiple Lines of Business. Under such circumstances, all affected Lines of Business must be part of the process. Effective SRM requires early and ongoing involvement by appropriate members of all affected FAA organizations. In the event that a disagreement arises among FAA organizations regarding SRM, the issue should be raised for resolution to the FAA Safety Management System Committee[1]. In the case where a hazard, its associated safety risk, and safety risk controls affect a single Line of Business, no further coordination beyond that Line of Business is necessary (excepting the provisions and requirements of FAA Order 1100.161 as they pertain to Air Traffic Safety Oversight).

2. Safety Risk Management Process. Hazards present conditions that affect operations in a way that results in degraded system performance, ultimately resulting in an unwanted outcome. A thorough understanding of the components of safety risk must entail an examination of the factors that increase or decrease the likelihood of system events (errors or failures) that can result in unwanted outcomes (accidents or incidents). The analysis must also consider the type of outcomes possible in order to estimate potential severity. It is recognized that a common taxonomy would facilitate

[1] The FAA SMS Committee was established in FAA Order 8000.369, *Safety Management System Guidance*.

effective communication across FAA organizations. Refer to FAA SRM Guidance[2] for more information regarding the taxonomy. The steps of the SRM process are described below.

a. System Analysis. The purpose of the system analysis step is to understand and describe the system to the extent necessary to identify potential hazards. It is a comprehensive approach to examining an issue in terms of what affects the issue and what the issue affects. A thorough system analysis is the foundation for conducting a sound safety analysis. The analysis provides information that serves as the basis to identify all hazards and their associated safety risk. When describing and analyzing the system, it is important to:

(1) Define and document the scope (i.e., system boundaries) and objectives related to the system.

(2) Develop a safety risk acceptance plan that includes: evaluation against safety risk acceptance criteria, designation of authority to make the required safety risk decisions involved, and assignment of the relevant decision-makers. Ensure consistency with Table 2-1: Risk Acceptance When Safety Risk Spans Lines of Business.

(3) Describe and model the system and operation in sufficient detail for the safety analysts to understand and identify the hazards that can exist in the system. For instance, modeling could entail creating a functional flow diagram to help depict the system and the interface with the users, other systems, or sub-systems.

(4) Look at the system in its larger context. A system is always a sub-component of some larger system(s). Therefore, a change to a system could impact the interfaces with these systems. If so, the SRM should address the effects on the interfaces or other systems, and/or coordinate with the owners of those other systems. For example, a change to the design of an aircraft may impact the maintenance and/or operation of that aircraft type.

(5) Consider the following in the analysis, depending on the nature and size of the system:

(a) Function and purpose of the system

(b) The system's operating environment

(c) An outline of the system's processes, procedures, and performance

(d) The personnel, equipment, and facilities necessary for the system's operation

b. Identify Hazards. During this step, consider the system analysis when identifying hazards. A hazard is a condition that could foreseeably cause or contribute to an accident. During the hazard identification step, hazards and the hazard's corresponding outcomes are identified and documented.

[2] FAA SRM Guidance is expected to be available by the end of fiscal year 2012.

c. Analyze Safety Risk.

(1) The objective of this step is to determine the initial safety risk of each identified hazard. The safety risk of a hazard is assessed on the combination of the severity of and the likelihood (probability) of the potential outcome(s) of the hazard. Where appropriate, existing controls are taken into account prior to safety risk determination. Appendix C – *Safety Risk Definition Tables and Risk Matrix* provides generic definitions for severity and likelihood to be used in this step of the process.

(2) When conducting safety analyses that cross Lines of Business, the analysis will be performed using the severity and likelihood tables of the Line of Business accepting the safety risk. If multiple Lines of Business will accept the safety risk and these Lines of Business cannot agree on which severity and likelihood definitions to use, the definitions documented in Appendix C of this order must be used.

(3) Regardless, of which definitions are used, this step includes the following common characteristics:

(a) The safety risk associated with the hazard must be determined and documented. The safety risk of a hazard is the function of the severity and likelihood of the hazard's potential outcomes.

1) Severity is the potential consequence or impact of a hazard in terms of degree of loss or harm. It is a prediction of how bad the outcome of a hazard can be. There may be many outcomes associated with a given hazard and the severity should be determined for each outcome.

2) Likelihood is the estimated probability or frequency, in quantitative or qualitative terms, of the outcome(s) associated with a hazard. It is an expression of how often an outcome of a hazard is predicted to occur in the future.

(b) Any assumptions made during the safety risk analysis should be documented, including the assumed exposure (e.g., life of the system, number of operations, operational hours).

(c) Any known limitations of the safety risk analysis should be described. Limitations may also include the margin of error of the analysis if it can be calculated.

d. Assess Safety Risk. In this step, each hazard's associated safety risk is plotted on the risk matrix based on the severity and likelihood of the outcome. The objective of this step is to determine the acceptability of the safety risk. A risk matrix provides a visual depiction of the safety risk and enables prioritization in the control of the hazards. Appendix C – *Safety Risk Definition Tables and Risk Matrix* provides a risk matrix to be used in this step of the process. However, if a hazard, its associated safety risk, and safety risk controls only affect one Line of Business, the Line of Business can use its existing safety risk assessment methodology and does not have to translate its assessment into the risk matrix in Appendix C. Please note that certain organizations in the FAA do not have definitions for severity categories below those that include fatalities (Hazardous and Catastrophic). These organizations can use their existing definitions and are not expected to develop definitions for the other categories.

e. Control Safety Risk.

(1) When safety risk is determined to be unacceptable, additional safety risk controls (to reduce the safety risk to an acceptable level) must be designed/developed and evaluated. The analysis is conducted to predict the residual risk as if the controls had been put in place. The prediction of the residual risk is assessed to determine if it meets the safety risk acceptance criteria. Further analysis is performed to ensure that no new hazards have been introduced or that existing safety risk controls have not been compromised based on the proposed safety risk controls. If the residual risk is not acceptable, the proposed safety risk controls are redesigned or new safety risk controls are developed as necessary and the analysis is reconducted.

(a) Controls should include a methodology for monitoring and tracking the predicted residual risk and assessing the safety risk against defined safety risk acceptance criteria.

(b) Safety risk controls established by the FAA must be approved by the FAA management official(s) responsible for their establishment before safety risk can be accepted. By approving a control, the management official agrees to establish the control as described in the SRM documentation.

(2) In cases in which controlling risk is outside the authority of the FAA (as described in Section 3c of this chapter), the FAA must document the analysis and decision, as well as apply the controls that it is able to and establish a methodology to monitor the risk.

3. Safety Risk Acceptance.

a. The appropriate management official accepts the safety risk associated with the identified hazard(s). When an individual or organization accepts safety risk, it does not mean that the risk is eliminated. Some safety risk remains; however, the individual or organization has determined that the prediction of the residual risk is acceptable. Each Line of Business must establish the levels of management that can accept safety risk based on the severity and likelihood. When the responsibility to manage the safety risk spans across Lines of Business, the residual risk must be accepted by the appropriate management official in each affected Line of Business.

b. Hazards may also be identified through the Safety Assurance monitoring of the system. In these situations, SRM should include a process for determining whether continued operation is acceptable (and for how long) while new safety risk controls are introduced. This process should include guidelines for managing elevated safety risk while developing a plan to reduce the safety risk. Each Line of Business must develop its own guidance and procedures for short-term acceptance of existing higher risk (that safety risk that is higher than would have been initially accepted) while working toward a mitigation plan to lower the safety risk. Table 2-1: *Risk Acceptance When Safety Risk Spans Lines of Business* summarizes the management levels for safety risk acceptance.

Table 2-1: Risk Acceptance When Safety Risk Spans Lines of Business*

Safety Risk Level	Risk Management Responsibility
Unacceptable	Unacceptable
Short-Term Acceptable	Associate Administrators of Lines of Business; ATO Chief Operating Officer**
Acceptable with Mitigation	Appropriate Level of Management in Each Affected Line of Business (as documented in risk acceptance plan)
Acceptable	Per Line of Business Guidance for Acceptable Risk

*Acceptance of risk may be delegated in accordance with FAA Order 1100.154, *Delegations of Authority*.
** The ATO Chief Operating Officer must comply with FAA Order 1100.161, *Air Traffic Safety Oversight.*

c. There are cases where hazards with significant associated safety risk may exist, but because of the constraints within which the FAA must operate, the FAA may not be able to establish controls. Such constraints include: the FAA's legal authority (which is established by statute), technological limitations, or cost-benefit requirements for regulations. Thus, the FAA may be forced to accept safety risk by default. When this is the case, the FAA must document the analysis and decision, as well as apply the controls that it is able to and establish a methodology to monitor the risk.

4. Safety Risk Monitoring and Hazard Tracking. Safety risk monitoring and hazard tracking include documenting safety risk controls, providing the status regarding validation and verification of safety risk controls, verifying implementation of safety risk controls, and updating the current and residual risk levels. Risk monitoring measures the effectiveness of safety risk control strategies. Monitoring of safety risk, depending on the circumstances, may range from failure tracking to alerts upon the occurrence of a specific outcome. Safety risk monitoring is primarily accomplished through the Safety Assurance functions. Hazard identification and tracking are foundational requirements for effective risk management. Hazard tracking is the process of tracking and managing the information regarding a hazard through the life-cycle of identification and iterations of assessment and control. While the agency develops a common hazard tracking system, each Line of Business shall ensure that it has processes and methods in place for safety risk monitoring and hazard tracking.

5. Documenting SRM Decisions.

a. Safety risk acceptance decisions made as a result of the safety risk analysis shall be recorded with the safety analysis documentation. Standardized documentation of safety risk acceptance facilitates consistent decision making and assists future decisions based on related analyses. The documentation should bring together the relevant information to enable the management official to understand the issue or system, its associated safety risk, and safety risk controls implemented (or proposed) to reduce the safety risk such that the residual risk is acceptable. The document must contain sufficient detail to enable the reader to comprehend what steps have been taken to identify safety issues and the corrective steps taken or proposed.

b. Each Line of Business must identify the process and documentation used to document the findings and results of each step of the SRM process. Although the documentation should be written to be understood by a reviewer familiar with the discipline(s) relevant to the issue or system (e.g., principal inspector or aircraft certification engineer), there should also be enough detail that a reviewer unfamiliar with the issue or system should also be able to understand the findings and any decisions made as a result.

c. At a minimum, the documentation must include:

(1) Identification of Individual or Team Who Conducted the Analysis.

(a) Name(s) and contact information

(b) Organization(s)

(c) Role of team member/individual in performing the analysis

(2) Description of the Issue and the Current System.

(a) An explanation of the trigger that resulted in undertaking the analysis

(b) A statement reflecting the impact of the issue or system (e.g., industry segment and level of impact such as local, regional, and national)

(c) Existing safety risk controls

(d) Pertinent interfaces and support systems required to maintain system function

(e) Reference to any other related analyses

(3) Identification of Hazards.

(a) Description of the hazards and how they were identified

(b) Existing controls related to the identified hazards

(4) Analysis of the Associated Safety Risk.

(a) Description of the hazard model used in the analysis including causes, system states, event(s), effects, and outcomes identified for each hazard

(b) Documentation of the identified safety risk including initial risk level (in terms of severity and likelihood) and when and how it appears in the current or proposed system

(c) Analytical basis and rationale for each of the above such as, but not limited to, historical data or other studies, modeling, simulation, experience with similar systems, or expert judgment

(d) Assumptions made and known limitations of the analysis including margin of error when it was calculated

(5) Analysis of Safety Risk Controls.

(a) Description of the safety risk controls that were considered

(b) Identification of selected safety risk control(s) and rationale including how the selected safety risk control(s) will mitigate the cause/effects of the hazard and, if applicable, expectations for implementation and compliance on the part of product/service providers affected by the decision and its associated safety risk controls

(c) Residual risk

1) A description of any remaining, unmitigated safety risk, including risk created by the proposed safety risk controls and strategies employed to mitigate/control this new safety risk

2) Description of how the hazards and their associated controls will be tracked and monitored against safety risk acceptance criteria

(6) Reviews and Approvals (if applicable).

(a) Description of any peer reviews conducted

(b) Signatures of management officials approving any safety risk controls and the safety analysis

(7) Risk Acceptance (if applicable).

(a) Name, position, and signature of manager(s)/executive(s) accepting the residual risk

(b) Rationale for acceptance of the safety risk. Examples for safety risk acceptance include:

1) Safety risk is below or equal to the threshold for acceptance

2) Other activities currently in development that would sufficiently reduce safety risk

3) Existing controls would sufficiently reduce safety risk, but are not being performed adequately (in this case, rationale should include a description of activities or actions which will be taken to assure risk controls are performed adequately in the future)

Chapter 3. Administrative Information

1. Distribution. This order is distributed to all offices in Washington Headquarters, regions, and centers, with distribution to all field offices and facilities.

2. Related Publications. This order has been developed to be consistent with the following documents:

a. FAA Order 8000.369, *Safety Management System Guidance*, September 30, 2009

b. FAA Order VS 8000.367, *Aviation Safety (AVS) Safety Management System Requirements*, May 14, 2008

c. FAA Order 1100.161, *Air Traffic Safety Oversight*, August 11, 2006

d. FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, March 19, 2007

e. FAA Order 5200.11, *FAA Airports (ARP) Safety Management System*, August 30, 2010

f. *Air Traffic Organization, Safety Management System Manual*, Version 2.1, May 2008

g. *Risk Analysis Specification, Version 2*, January 21, 2009

h. AC 431.35-1, *Expected Casualty Calculations for Commercial Space Launch and Reentry Missions*, August 30, 2000

i. *Safety Approval Guide for Applicants, Version 1.0*, September 28, 2009

j. FAA Order 1100.154*A*, *Delegations of Authority*, June 12, 1990

k. *International Civil Aviation Organization Annexes 1, 6, 8, 11, 13, and 14*

l. *ICAO Safety Management System Manual* (Document 9859), 2nd Edition, 2009

m. *Joint Planning and Development Office (JPDO), Safety Management System Standard v1.4*, July 30, 2008

3. Authority to Change This Order. The FAA Administrator has authority to issue changes and revisions to this order.

Appendix A – Definitions

a. Accident – An unplanned event or series of events that results in death, injury, or damage to, or loss of, equipment or property.

(1) Aircraft Accident – An occurrence associated with the operation of an aircraft that takes place between the time any person boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage.

b. Aerospace System – U.S. airspace, all manned and unmanned vehicles operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, pilots, regulations, policies, procedures, facilities, equipment, and all aviation-related industry.

c. Analysis – The process of identifying a question or issue to be addressed, examining the issue, investigating the results, interpreting the results, and possibly making a recommendation. Analysis typically involves using scientific or mathematical methods for evaluation.

d. Assessment – Process of measuring or judging the value or level of something.

e. Control – *See Safety Risk Control.*

f. Hazard – A condition that could foreseeably cause or contribute to an accident.

g. Incident – An occurrence other than an accident that affects or could affect the safety of operations.

h. Likelihood – The estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome.

i. Mitigation – A means to reduce the risk of a hazard. *See Safety Risk Control*.

j. Risk – *See Safety Risk.* The terms *Risk* and *Safety Risk* are used synonymously.

k. Safety – The state in which the risk of harm to persons or property damage is acceptable.

l. Safety Assurance – Processes within the SMS that function systematically to ensure the performance and effectiveness of safety risk controls and that the organization meets or exceeds its safety objectives through the collection, analysis, and assessment of information.

m. Safety Risk – The composite of predicted severity and likelihood of the potential effect of a hazard.

(1) Initial – The predicted severity and likelihood of a hazard's effects or outcomes when it is first identified and assessed; includes the effects of preexisting risk controls in the current environment.

(2) Current – The predicted severity and likelihood at the current time.

(3) Residual – The remaining predicted severity and likelihood that exists after all selected risk control techniques have been implemented.

n. Safety Risk Control – A means to reduce or eliminate the effects of hazards.

o. Safety Risk Management (SRM) – A process within the SMS composed of describing the system, identifying the hazards, and analyzing, assessing, and controlling risk.

p. Severity – The consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm.

q. System – An integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets.

Appendix B – Acronyms

a. **AIR** – Aircraft Certification

b. **ANG** – NextGen Organization

c. **ARP** – Airports Organization

d. **AST** – Commercial Space Transportation Organization

e. **ATO** – Air Traffic Organization

f. **AVS** – Aviation Safety Organization

g. **ICAO** – International Civil Aviation Organization

h. **JPDO** – Joint Planning and Development Office

i. **NAS** – National Airspace System

j. **SMS** – Safety Management System

k. **SRM** – Safety Risk Management

l. S**SP** – State Safety Program

Appendix C – Safety Risk Definition Tables and Risk Matrix

1. The severity and likelihood definition tables in this Appendix are used in the Analyze Safety Risk step of SRM. These definitions are generic definitions. Each affected Line of Business may develop more specific definitions for use in its application of SRM.

2. It is important to recognize that an identified hazard can result in more than one outcome, and that these outcomes have different levels of severity and probabilities of occurrence. To facilitate this evaluation, all credible system states should be considered. The probability of an outcome may be known to be so low (compared to Line of Business guidance) that it does not need to be considered. Additionally, recognize that the highest safety risk may not be associated with the worst credible outcome.

3. The definitions are not meant to imply a specific point, but instead, convey a spectrum across the cells from very low to very high (either severity or likelihood). Additionally, even within each cell there is a range (of severities and likelihoods) which lies between the ranges described in the cells before and after it.

Table C-1: Severity Definitions*

Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
Negligible safety effect	– Physical discomfort to persons – Slight damage to aircraft/vehicle	– Physical distress or injuries to persons – Substantial damage to aircraft/vehicle	Multiple serious injuries; fatal injury to a relatively small number of persons (one or two); or a hull loss without fatalities	Multiple fatalities (or fatality to all on board) usually with the loss of aircraft/ vehicle

* Excludes vehicles, crew, and participants of commercial space flight.

Table C-2: Likelihood Definitions

Frequent **A**	Expected to occur routinely
Probable **B**	Expected to occur often
Remote **C**	Expected to occur infrequently
Extremely Remote **D**	Expected to occur rarely
Extremely Improbable **E**	So unlikely that it is not expected to occur, but it is not impossible

The risk matrix below is used in the Assess Safety Risk step of SRM.

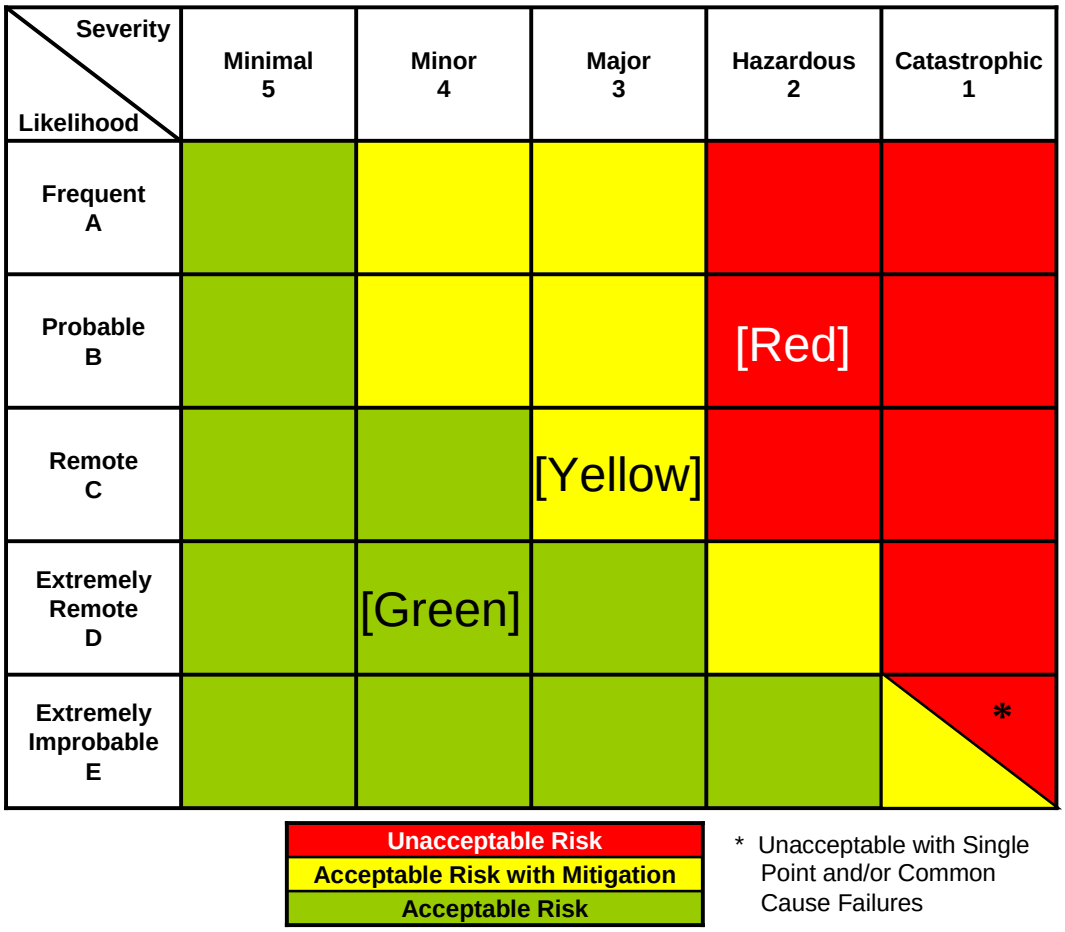

Figure C-1: Risk Matrix

4. A risk matrix is a graphical means of determining safety risk levels. The columns in the matrix reflect previously introduced severity categories; its rows reflect previously introduced likelihood categories. This matrix is intended as a standardized baseline to facilitate communication across FAA organizations.

5. In addition, some FAA organizations have existing safety risk assessment processes to determine safety risk levels without using a risk matrix (for example, evaluation against the probability of a fatal outcome). Since there is obvious overlap, the risk matrix may be useful in communication between Lines of Business. The risk matrix is a tool that facilitates communication regarding safety risk among the FAA organizations through the graphical illustration of safety risk analysis and assessment results. Using the risk matrix across the Lines of Business does not preclude organizations from using their own means of analyzing and assessing safety risk. It also does not preclude organizations from using methodologies or frameworks other than the risk matrix to illustrate and communicate the results of those analyses and assessments within a Line of Business. Therefore, if a hazard, its associated safety risk, and safety risk controls stay within a Line of Business, the Line of Business may use its existing safety risk assessment methodology. It does not have to translate its assessment

into the risk matrix included in this document. When the team conducting the analysis is comprised of members from Lines of Business that use different risk matrices, the team uses the risk matrix in this policy. In cases in which controlling risk is outside the authority of the FAA (as described in Chapter 2, Section 3c of this policy) the FAA must document the analysis and decision, as well as apply the controls that it is able to and establish a methodology to monitor the risk.

6. The risk levels used in the process are defined below.

a. **Unacceptable** – This is unacceptable safety risk and it cannot be accepted by any level of management until it has been mitigated to an acceptable level.

b. **Short-Term Acceptable –** That safety risk that is higher than would have been initially accepted, but is allowed to exist while new safety risk controls are developed and implemented.

c. **Acceptable with Mitigation** – This safety risk is acceptable, however mitigation, tracking, and monitoring are required.

d. **Acceptable** – This safety risk is acceptable without restriction or limitation; hazards are not required to be actively managed, but must be documented.

7. Using the risk matrix, each hazard is ranked and prioritized according to its associated safety risk levels following the steps below:

a. When appropriate, rank hazards according to their associated safety risk levels (illustrated by where they fall on the risk matrix).

b. To plot a hazard on the risk matrix, select the appropriate severity column (based on the severity definitions) and move down to the appropriate likelihood row (based on the likelihood definitions).

c. Plot the hazard in the box where the severity and likelihood of the effect or outcome associated with the hazard meet.

d. If this box is red, the safety risk associated with the hazard is unacceptable; if the box is yellow, the safety risk associated with the hazard is acceptable with mitigation; if the box is green, the safety risk associated with the hazard is acceptable.

e. Once mitigations are developed and the analysis is conducted taking into account those mitigations, the residual risk is plotted. Plotting the prediction of the residual risk illustrates the impact of the safety risk controls on the initial risk and shows the decision-maker whether or not the safety risk associated with the hazard will be mitigated to an acceptable level.

8. Ranking the safety risk associated with the identified hazards prioritizes mitigation.