



U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
National Policy

ORDER
8040.4B

Effective Date:
05/02/17

SUBJ: Safety Risk Management Policy

This order supports Federal Aviation Administration (FAA) Order 8000.369, *Safety Management System*, and establishes requirements for how to conduct Safety Risk Management (SRM) in the FAA. It formalizes SRM guidance for FAA Lines of Business (LOBs) and Staff Offices, and describes specific steps when performing and documenting SRM.

The FAA's mission is to provide the safest, most efficient aerospace system in the world. In support of this mission, the FAA uses a Safety Management System (SMS) to integrate the management of safety risk into operations, acquisitions, rulemaking, and decision making. The SMS enhances the safety of the flying public and strengthens the FAA's worldwide leadership in aviation safety.

The SMS consists of four components: Safety Policy, SRM, Safety Assurance, and Safety Promotion. The objective of SRM is to provide information regarding hazards, safety risk, and safety risk controls/mitigations to decision makers and to enhance the FAA's ability to address safety risk in the aerospace system. SRM consists of conducting a system analysis; identifying hazards; and analyzing, assessing, and controlling safety risk associated with the identified hazards. SRM as described in this order outlines standardized principles that enhance the FAA's ability to coordinate risk-based decision making across organizations. Safety Policy and Safety Promotion are not addressed in this order, but are discussed in detail in FAA Order 8000.369, *Safety Management System*. However, Safety Assurance is described in this order due to its importance in triggering SRM through the identification of potential hazards or ineffective safety risk controls, as well as its role in monitoring safety risk controls. All four components work together to enable the FAA to manage safety within the aerospace system.

A handwritten signature in black ink, appearing to read "Michael P. Huerta", is written over a circular stamp or seal.

Michael P. Huerta
Administrator

Table of Contents

Chapter 1. General Information.....	3
1. Purpose of This Order.....	3
2. Audience.....	3
3. Where You Can Find This Order.	3
4. Cancellation.	3
5. Explanation of Changes.....	3
6. Background.....	4
7. Scope.	5
Chapter 2. Conducting Safety Risk Management	7
1. General Information.	7
2. Safety Risk Management Process.	12
3. Safety Risk Acceptance.	16
4. Safety Performance Monitoring and Hazard Tracking.....	18
5. Documenting Assessments and Decisions.	19
Chapter 3. Administrative Information.....	22
1. Distribution.....	22
2. Related Publications.	22
3. Authority to Change This Order.	22
Appendices.....	A-1
Appendix A. Definitions.....	A-1
Appendix B. Acronyms	B-1
Appendix C. Safety Risk Definition Tables and Risk Matrix	C-1
Appendix D. Disclosure for FAA Personnel to Participate on SRM Teams.....	D-1

Chapter 1. General Information

1. Purpose of This Order. This order establishes the Safety Risk Management (SRM) policy for the Federal Aviation Administration (FAA). It also establishes common terms and processes used to analyze, assess, mitigate, and accept safety risk in the aerospace system. 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 how SRM is conducted and the tools and techniques that are employed. However, the process requires consistency in the application of SRM principles. Appendix A, *Definitions*, contains definitions for terms used in this policy. Appendix B, *Acronyms*, contains acronyms used in this policy.

2. Audience. This order applies to the following Lines of Business (LOBs): the Air Traffic Organization (ATO), the Aviation Safety Organization (AVS), the Office of Airports (ARP), the Office of Commercial Space Transportation (AST), and the Office of Security and Hazardous Materials Safety (ASH), as well as the Office of the Next Generation Air Transportation System (ANG), which is a Staff Office. This order is written to be broadly applicable to the aerospace system, which would allow it to be applied to other FAA organizations in the future, if management determines broader application to be appropriate.

3. Where You Can 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 8040.4A, *Safety Risk Management*, dated April 30, 2012, and FAA Notice 8000.374, *Hazard Identification, Risk Management & Tracking (HIRMT) Tool Implementation*, dated January 29, 2016.

5. Explanation of Changes. This revision does the following:

- a. Adds requirements regarding the use of HIRMT.
- b. Revises safety risk levels and safety risk acceptance criteria.
- c. Includes additional definitions in Appendix A and additional acronyms in Appendix B.
- d. Provides new likelihood definitions and updates the risk matrix to support safety risk assessments in Commercial Operations/Large Transport Category in Appendix C, *Safety Risk Definition Tables and Risk Matrix*.
- e. Provides new likelihood definitions and a new risk matrix to support safety risk assessments in General Aviation Operations/Small Aircraft and Rotorcraft in Appendix C.
- f. Includes information regarding conducting SRM with entities outside the FAA and a disclosure form to be used by FAA employees to participate on SRM Teams established and led by entities outside the FAA in Appendix D, *Disclosure for FAA Personnel to Participate on SRM Teams*.

6. Background.

a. The FAA's mission is to provide the safest, most efficient aerospace system in the world. In support of this mission, the FAA uses a Safety Management System (SMS) to integrate the management of safety risk into operations, acquisition, rulemaking, and decision making. The SMS enhances the safety of the flying public and strengthens the FAA's worldwide leadership in aviation safety. As described in FAA Order 8000.369, *Safety Management System*, the SMS consists of four components: Safety Policy, SRM, Safety Assurance, and Safety Promotion. These components work together to enable the FAA to manage safety within the aerospace system.

b. This order establishes the SRM policy for the FAA. This SRM policy supports the FAA SMS by providing the ability to consistently conduct SRM and provide safety risk information to decision makers. Further, along with Safety Assurance functions, SRM assists the FAA in ensuring that hazards are identified and the safety risk associated with those hazards is managed to acceptable levels throughout the aerospace system. To manage safety risk, controls or mitigations are used to reduce or eliminate the effects of identified hazards. The terms *control*, *mitigation*, and *safety risk control* are used synonymously in this document.

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 includes both regulatory and product/service provider organizations, the FAA chose to implement an SSP and an SMS. The FAA SMS meets most of the tenets of both the ICAO SSP and SMS frameworks, thereby ensuring interoperability among safety management functions across FAA organizations.

(1) The FAA as Regulator. Regulators perform rulemaking, certification, operational oversight, and continued operational safety functions. Therefore, they provide regulatory oversight of the aerospace system. As such, regulators do not own the systems/operations; rather, the product/service providers own and control their operations. Within the limits of the regulator's authority, regulators can apply controls to product/service provider activities and operations. These controls are promulgated through regulations, standards, policy, approvals, guidelines, etc., which are the output of the regulator's SRM activities. The actual implementation of the safety risk mitigation rests with the product/service provider. However, the regulator does conduct SRM when regulations (or other safety risk controls within its purview) are created, modified, or removed. Hazards with significant associated safety risk may exist, but because of the limitations within which the regulator must operate, the regulator may not be able to establish controls sufficient to mitigate the safety risk to an acceptable level. Such limitations include the regulator's legal authority (which is established by statute and executive order), technological limitations, cost-benefit requirements for regulations, and the lack of cost-effective solutions. When this is the case, the regulator must document the analysis and/or assessment, any decisions made, and the rationale for those decisions. The regulator must also apply the controls that it is able to, and establish a methodology to monitor the safety risk. In general, FAA organizations that are regulators do not perform SRM on behalf of individual product/service providers. Rather, the product/service provider is responsible for conducting their own SRM. A regulator may conduct an independent assessment to validate a product/service provider's assessment or, simply, to have an independent view of the issue/concern. Additionally, the FAA may need to facilitate SRM in situations where the safety risk owner is unable or unwilling to do so.

(2) The FAA as Product/Service Provider. Product/service providers are organizations engaged in the delivery of aviation products or services. When an FAA organization is performing in the capacity of a product/service provider, it is responsible for conducting SRM and applying mitigations because it has the ability to directly control safety risk in its operations. Specifically, it owns the personnel, processes, equipment, and systems to provide a product or service. A product/service provider can even, if necessary, cease operations in certain environments, discontinue use of some systems, alter the configurations or operating practices of their systems, etc.

(3) The FAA's Role in Other Federal Actions. Certain FAA LOBs perform functions such as developing standards, approvals, and oversight. These functions are typically required by statute or executive order, not regulation. While not directly addressed in the ICAO SMS framework, the FAA must ensure that safety risk of any hazards associated with these activities is acceptable. SRM provides LOBs an additional tool to assist in performing these functions. For example, ARP must approve certain development activities before an airport service provider can begin construction. While there is an expectation that the service provider will conduct SRM on the development project, the FAA may need to conduct its own SRM in addition to other evaluations to adequately assess the proposed project before approval. In this case, the appropriate FAA LOB would lead the SRM activity with assistance from other impacted LOBs or Staff Offices and applicable industry representatives.

7. Scope.

a. This order supports the current version of FAA Order 8000.369, *Safety Management System*, and it describes the principles used to guide SRM within the FAA. It formalizes the use of SRM across the FAA, describes the specific steps when performing SRM, and enables communication and coordination across FAA organizations for enhanced safety risk decision making. In general, the scope of the assessment is a function of the nature, complexity, and consequence of the identified issue. The scope and complexity of the safety assessment should be tailored to the issue or change being analyzed. In addition, limits in data availability may necessitate a less quantifiable approach and/or result than when data is available. However, regardless of the scope and complexity, the intent of the SRM process is to provide safety information as an input to decisions so that resources can be focused on addressing areas with the highest safety risk in a timely manner.

b. This order requires the use of HIRMT for Aerospace System Level (ASL) safety issues. Chapter 2, subparagraphs 4b-e describe HIRMT and the criteria for ASL safety issues.

c. This order establishes a standard approach for SRM that enables communication and coordination across FAA organizations for enhanced safety risk decision making. Safety risk assessments and controls that cross organizations must be fully coordinated among the affected organizations. The FAA SMS Committee is a resource for organizations to work through when trying to coordinate safety issues across LOBs or Staff Offices.¹ 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. Documenting the assessment to include what was considered, as well as the rationale for the findings and any resultant

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

decisions, is an important step in the process and will help facilitate better communication and coordination. Chapter 2, paragraph 5 describes documentation of assessments and decisions.

Chapter 2. Conducting Safety Risk Management

1. General Information.

a. Introduction. SRM is one of the four components of the SMS that enables 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 critical information for decision makers by identifying hazards, analyzing safety risk, assessing safety risk, and developing controls to reduce safety risk to an acceptable level. SRM facilitates communication and coordination across FAA organizations for enhanced safety risk decision making.

c. Applicability. In general, SRM is conducted when making planned changes to the aerospace system and when potential and previously unidentified hazards and/or ineffective risk controls are discovered. SRM is used to evaluate the need for, as well as develop, safety risk controls in the aerospace system. Effective SRM requires early and ongoing involvement by appropriate stakeholders. Each applicable organization (listed in the Audience section) 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.

d. Relationship Between SRM and Safety Assurance.

(1) While the focus of this policy is on SRM, it is important to understand how the SRM and Safety Assurance functions work together within an SMS. The SRM process provides a system analysis, the identification of hazards, and the analysis and assessment of safety risk. When appropriate, safety risk controls are developed and, once they are determined to be practicable in mitigating safety risk to an acceptable level, employed operationally. Safety Assurance is used to ensure the safety risk control strategies that have been employed are achieving their intended safety risk mitigation objectives. If the controls are not adequately mitigating 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 using Safety Assurance functions, which are then analyzed and assessed using SRM.

(2) The FAA uses Safety Assurance functions to monitor aerospace system data to determine the existence of potential hazards, ineffective safety risk controls, or instances of nonconformance with requirements intended to control safety risk. The FAA implements systems and procedures and applies expertise to use Safety Assurance to identify hazards in the aerospace system. Safety Assurance functions are discussed in this order because this activity feeds and follows SRM. While the Safety Assurance functions generally follow the flow shown in Figure 2-1, *SRM and Safety Assurance Processes*, the functions may not be performed in the sequence as illustrated. For the purposes of illustration, this order will describe Safety Assurance as shown generically in Figure 2-1.

(a) System Operation. This represents the entire aerospace system in operation.

(b) Data Acquisition and Process. This function includes data regarding the operation of the aerospace system, including the performance of safety risk mitigations, that is acquired and stored for analysis by the FAA. Data sources external to the FAA such as industry or international organizations should also be considered and used when it is available and it can be validated.

(c) Data Analysis. Data analysis is conducted on the data acquired to assess system performance, identify potential hazards (including frequency of events), measure the effectiveness of safety risk controls (i.e., safety performance targets identified in monitoring plans are met), and identify instances of nonconformance.

(d) System Assessment. The system assessment is based on the data analysis to identify potential new hazards or ineffective safety risk controls (i.e., safety performance targets identified in monitoring plans are not met) and determine conformance with requirements. FAA organizations may use a variety of tools and techniques to conduct the system assessment. Three possible outcomes of the system assessment are:

1) When a potential hazard or ineffective control is identified, FAA organizations will initiate SRM.

2) When the system is determined to be in conformance with requirements and standards, FAA organizations may continue operation.

3) When a nonconformance is identified, further action may be taken.

(e) Corrective Action. When an instance of nonconformance is identified, FAA organizations investigate and may implement corrective action(s), which might require SRM.

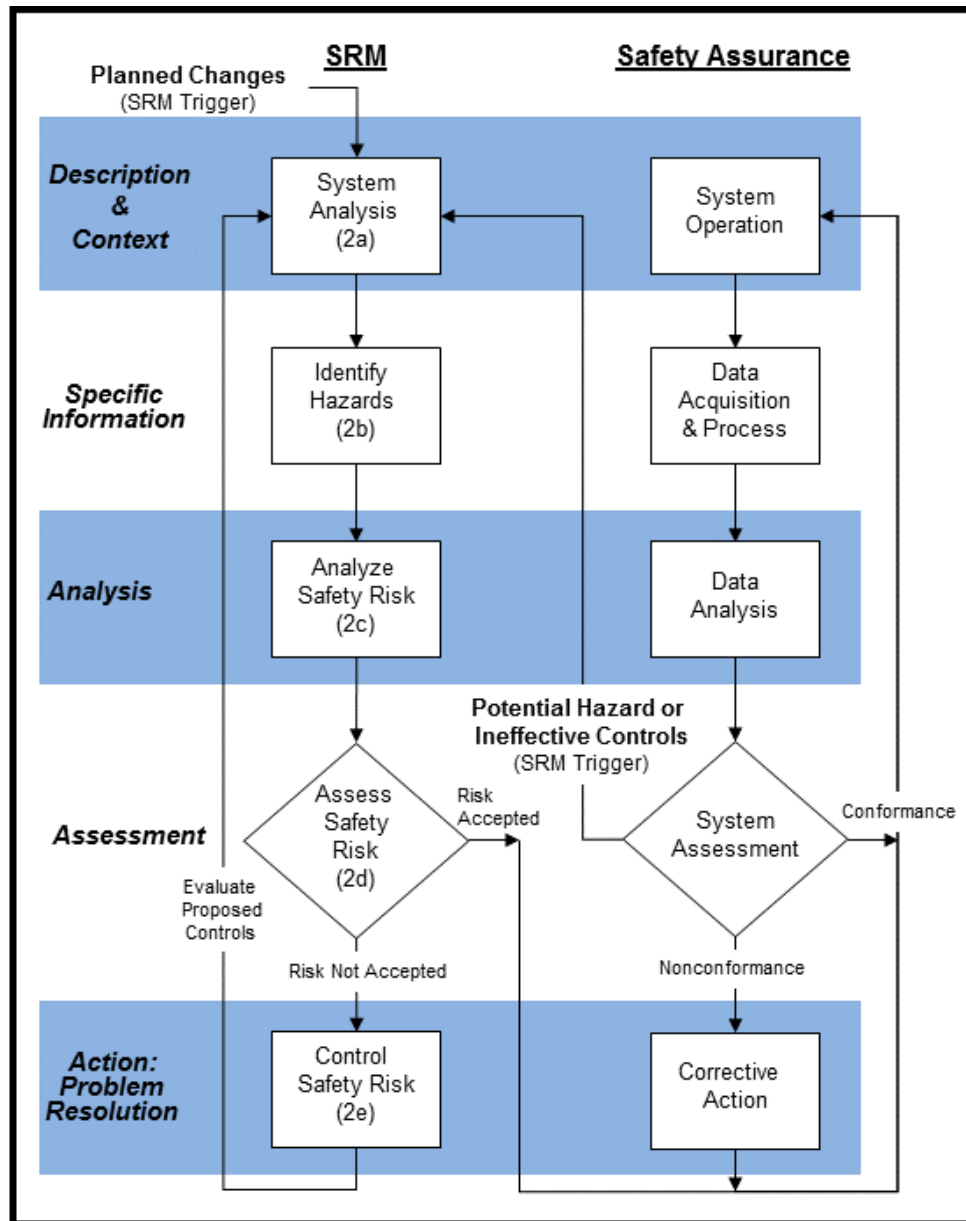


Figure 2-1: SRM and Safety Assurance Processes

e. Triggers. There are two basic triggers for applying SRM. The first is planned changes, and the second is discovery of potential hazards or ineffective controls from the Safety Assurance process, as shown in Figure 2-1.

f. 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 in evaluating safety in the operational environment. There are additional considerations for SRM in the operational environment. Operational data provides 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. Analysis and assessment processes may uncover safety risk that would not have met risk acceptance criteria when the product or system was first put into service. This can present a difficult situation, especially if controls to mitigate the risk associated with the newly identified hazard require changes that cannot be immediately implemented. For this reason, SRM in the operational environment often necessitates allowing safety risk to exist in the system that is higher than would have been initially accepted while controls are being developed and implemented to lower the safety risk. For example, the Aircraft Certification Service (AIR) has acceptable safety risk guidelines for continued operation in the short term. AIR also has safety risk guidelines for acceptable operations in the long term that may be different from those used for initial certification. In this context, short term does not refer to a specific time period (for example, “90 days” or “1 year”); rather, it refers to the period of time during which the safety risk of the hazard does not exceed the guidelines for continued operation.

g. Office of Primary Responsibility. The Office of Primary Responsibility (OPR) for SRM is the organization that manages and tracks the issue or change through closure. The OPR’s responsibilities include leading and managing the safety risk assessment, identifying the appropriate management officials to accept safety risk and approve mitigations, coordinating any necessary approvals and safety risk acceptance decisions, and tracking and monitoring any approved risk mitigations. The OPR is also responsible for entering results and decisions into HIRMT, if required, and updating the information in HIRMT, as necessary, to provide status based on the monitoring plan (for more information regarding HIRMT, please see Chapter 2, subparagraph 4). The OPR is typically the office with the certification or responsibility for the issue or change under consideration. Ultimately, assignment of the OPR or acceptance of the responsibility is a management decision and is typically the result of discussion and agreement amongst the stakeholder organizations.

h. FAA SMS Committee. The FAA SMS Committee, on behalf of the SMS Executive Council, provides a forum for organizations to coordinate SRM activities across LOBs and Staff Offices when appropriate.² Organizations can raise safety issues to the FAA SMS Committee when an organization determines that the issue would best be addressed cross-organizationally. After review, the FAA SMS Committee determines whether to track and manage the safety issue on behalf of the FAA SMS Executive Council. In this case, SRM is conducted by cross-organizational SRM Teams in order to most efficiently and effectively use safety management resources. The FAA SMS Committee has authority to assign the OPR for safety risk assessments that it manages and tracks on behalf of the FAA SMS Executive Council. The OPR is responsible for coordinating with the FAA SMS Committee to determine when the assessment is complete and/or when the issue can be closed.

i. SRM Responsibilities.

(1) Depending on the issue or change 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 should be formed to adequately address the scope and complexity of the issue. In order to be most useful to decision makers, SRM is best conducted by an individual who has, or a

² For more information regarding the FAA SMS Committee and FAA SMS Executive Council, please refer to the latest version of FAA Order 8000.369.

team whose members have, a diverse set of skills. Multiple disciplines should be represented on these teams, including those with expertise in the system or operation being analyzed, as well as technical, engineering, and safety areas. SRM Teams³ must include representatives from the various organizations that could be affected by the issue or change under consideration, which often means that multiple LOBs and/or Staff Offices will be represented. SRM Team members do not make safety risk acceptance decisions, which is a management function; however, they are responsible for coordinating the results of the assessment within their organization and with their management, as appropriate. To ensure the quality of participation from team members, it is important that all team members have a basic understanding of SRM prior to commencing the SRM Team meetings.

(2) Peer review is encouraged to strengthen decision maker confidence in the findings. Individuals, other than those who have conducted SRM, should perform the peer reviews. These individuals should have similar expertise as the SRM Team members. The FAA SMS Committee reviews safety risk assessments that it tracks and manages on behalf of the FAA SMS Executive Council.

j. Coordination Among LOBs. A safety issue may affect multiple LOBs and/or Staff Offices. Under such circumstances, all affected FAA organizations 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 that cannot be resolved, the issue should be raised for resolution to the FAA SMS Committee. In the case where a hazard, its associated safety risk, and safety risk controls affect a single LOB or Staff Office, no further coordination beyond that LOB or Staff Office is necessary (excepting the provisions and requirements of the current version of FAA Order 1100.161, *Air Traffic Safety Oversight*, as they pertain to the Air Traffic Safety Oversight Service (AOV)).

k. Coordination With Stakeholders Outside the FAA.

(1) FAA Participation on SRM Teams Established and Led by Outside Entities. There are many instances when the FAA may be asked to participate on SRM Teams established and led by entities outside the FAA, including product/service provider organizations for which the FAA has oversight responsibilities. The FAA employee participating on an SRM Team established and led by entities outside the FAA must provide that organization with the Disclosure in Appendix D of this order. The FAA representative must request that an authorized representative of the organization acknowledge receipt of the disclosure by signing and dating it. FAA personnel will properly document the signed disclosure in accordance with the policies and guidance for their organization. In accordance with the disclosure, FAA employees' participation on an SRM Team established and led by entities outside the FAA does not constitute the FAA's endorsement of the findings of the SRM Team. Therefore, FAA personnel participating on the SRM Team should not concur with any document, recommendation, or other product developed by the SRM Team. If the outside entity wishes to obtain FAA concurrence, it should be advised to submit the product to the FAA for review.

³ An SRM Team is a cross-organizational group that is established to conduct SRM on issues that affect more than one FAA organization. An SRM Team is roughly equivalent to an SRM Panel. However, an SRM Team is cross organizational, while an SRM Panel may or may not be cross organizational.

(2) Outside Entity Participation on SRM Teams Established and Led by the FAA. In order to conduct a thorough assessment, it is important to have all necessary expertise on the SRM Team. At times, this means that the FAA might request participation from entities outside the FAA, including product/service provider organizations for which the FAA has oversight responsibility. In such cases, it is advisable that the OPR consult with the appropriate official or organization in the FAA regarding data protection and Freedom of Information Act (FOIA) requirements. This is especially advisable if the SRM Team will have access to data/information that is not publicly available. In addition, the OPR should confer with the FAA Office of the Chief Counsel (AGC) to avoid any potential legal/statutory issues.

2. Safety Risk Management Process.⁴ 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. The steps of the SRM process are described below. While the steps of the process are described sequentially, they may be accomplished in parallel. The SRM requirements and concepts described in this order do not preclude FAA organizations from taking immediate interim action to mitigate existing safety risk prior to conducting SRM and identifying permanent mitigations.

a. System Analysis.⁵ 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 or change in terms of what it affects and what is affected by the issue or change. A thorough system analysis is the foundation for conducting a sound safety analysis. The system analysis provides information that serves as the basis for identifying and understanding hazards, as well as their causes and 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) Gather the relevant available data/information regarding the issue or change to be analyzed. This includes available incident/accident data; previous applicable analyses and assessments; and related requirements, rules, and regulations, as necessary.

(3) 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, ensuring consistency with Table 2-1, *Safety Risk Acceptance Criteria for Issues or Changes That Cross LOBs/Staff Offices* (see Chapter 2, subparagraph 3b). If an organization does not have risk acceptance criteria, a combination of Table 2-1 and the risk matrices and definitions provided in Appendix C may be used. It is acknowledged that some parts of the risk acceptance plan may need to be updated based on the results of later steps in the

⁴ Please refer to the SMS page on the FAA Intranet for additional guidance regarding SRM, which is available at: https://my.faa.gov/tools_resources/safety_initiatives/sm/sms/srm.html.

⁵ A system is defined as 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.

process (for instance, the designation of authority to make risk acceptance decisions may need to be updated depending on the proposed safety risk mitigations).

(4) 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, as well as their sources and possible outcomes. One example of modeling is creating a functional flow diagram to help depict the system and the interface with the users, other systems, or subsystems.

(5) Look at the system in its larger context. A system is often a subcomponent of some larger system(s). Therefore, a change to a system could affect the interfaces with these systems. 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 affect the maintenance and/or operation of that aircraft type.

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

- (a) The function and purpose of the system;
- (b) The system's operating environment;
- (c) An outline of the system's processes, procedures, and performance; and
- (d) The personnel, equipment, and facilities necessary for the system's operation.

b. Identify Hazards.⁶ When identifying hazards in this step, consider the system analysis. A hazard is a condition that could foreseeably cause or contribute to an aircraft accident. During the hazard identification step, hazards and each hazard's corresponding outcomes are specifically identified and documented. The hazard identification step considers all reasonably possible sources of hazards. Remember that elements in the system analysis may be sources of hazards. The Bow-Tie method or Bow-Tie diagram is an example of a tool that can be used to assist in the identification of hazards. Again, the elements in the system analysis may all be sources of hazards. Depending on the nature and size of the system under consideration, these could include:

- (1) Ambient environment (physical conditions, weather, etc.);
- (2) Equipment (hardware and software);
- (3) External services (contract support, electric, telephone lines, etc.);
- (4) Human-machine interface;
- (5) Human operators;
- (6) Maintenance procedures;

⁶ If no hazards are identified, the findings should be documented and reported to the OPR who will determine the next steps for the issue or change being analyzed.

- (7) Operating environment (airspace, air route design, etc.);
- (8) Operational procedures;
- (9) Organizational culture;
- (10) Organizational issues; and
- (11) Policies/rules/regulations.

c. Analyze Safety Risk.

(1) The objective of this step is to determine the initial safety risk associated with the effects of each identified hazard. The safety risk associated with a hazard is the combination of the severity and the likelihood of the potential outcome(s) of the hazard. Where appropriate, existing controls are taken into account prior to safety risk determination.

(2) When conducting safety analyses that cross LOBs, the analysis will be performed using the risk analysis and assessment process of the LOB accepting the safety risk.⁷ If multiple LOBs will accept the safety risk and these LOBs cannot agree on which severity and likelihood definitions to use, the definitions and risk matrices documented in Appendix C should be considered for use, as appropriate, or advice from the FAA SMS Committee should be sought to resolve differences.

(3) When a hazard, its associated safety risk, and safety risk controls stay within an LOB or Staff Office, the FAA organization may use its existing safety risk analysis methodologies (including severity and likelihood definitions, if applicable).

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

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

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. When sufficient empirical data exists, statistical probabilities should be used.

(b) In general, the SRM Team should limit assumptions as much as practical. If any assumptions are made, the assumptions and their rationale must be documented.

⁷ For more information regarding safety risk acceptance, please refer to Chapter 2, subparagraph 3.

(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 assessed against the risk acceptance criteria identified in the safety risk acceptance plan and plotted on a risk matrix based on the severity and likelihood of the outcome. The objective of this step is to determine the safety risk level acceptability. A risk matrix provides a visual depiction of the safety risk and enables prioritization in the control of the hazards. Appendix C provides risk matrices to be used in this step of the process. If a hazard's associated safety risk and/or safety risk controls only affect one LOB or Staff Office, the organization can use its existing safety risk assessment methodology, and it does not have to translate its assessment into the risk matrix in Appendix C. 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) Additional safety risk controls (to reduce the safety risk to a level acceptable to the decision maker) may need to be designed/developed and evaluated by the team or individual conducting the assessment. The analysis is conducted to predict the residual safety risk as if the proposed controls had been put in place. The prediction of the residual safety risk is assessed to determine if the safety risk acceptance criteria are met. If an organization does not have risk acceptance criteria, a combination of Table 2-1 and the risk matrices and definitions provided in Appendix C may be used (see Chapter 2, subparagraph 2a(3)). 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. This is done until the proposed safety risk controls enable the safety risk acceptance criteria to be met.

(2) Safety risk controls established by the FAA must be approved by the FAA management officials who are responsible for their implementation before safety risk can be accepted. By approving a control, the management official agrees to establish the control as described in the SRM documentation. The OPR is responsible for obtaining necessary approval(s) and safety risk acceptance(s) after the safety risk assessment and development of proposed safety risk controls are complete. The appropriate management officials either approve the proposed safety risk mitigations/controls within their purview or send the assessment back for additional analysis or identification of additional proposed alternatives for safety risk mitigations/controls. Note that the management officials who approve the safety risk controls may be the same management officials who accept the safety risk, but this is not always the case.

(3) In cases in which controlling safety risk is outside the authority of the FAA (as described in subparagraph 3c of this chapter), the FAA must document the assessment and decision, as well as apply the controls that it is able to and establish a methodology to monitor the safety risk. When possible, the FAA should identify if another organization(s) is in a position to implement safety risk controls. If another organization(s) is in a position to do so, the FAA should seek to enter into agreement(s) with the organization(s) to implement and monitor the safety risk controls, if possible.

There may also be circumstances in which there is not enough information to determine the appropriate risk control strategies. In these circumstances, the FAA must document the assessment and any decisions made, as well as establish a methodology to monitor the safety risk and establish a plan to collect the necessary data and reassess the issue at a later time.

3. Safety Risk Acceptance.

a. Once the assessment is complete and the findings and alternatives/proposals for safety risk mitigations/controls are documented, the results are delivered to the appropriate management official within the OPR. The OPR is responsible for obtaining necessary approval(s) and safety risk acceptance(s). The appropriate management officials either accept the safety risk associated with the identified hazard(s) within their purview or they send the assessment back for additional analysis or identification of additional proposed alternatives for safety risk mitigations/controls. When an individual or organization accepts safety risk, it does not mean that the safety risk is eliminated. Some safety risk remains; however, the individual or organization has determined that the prediction of the residual safety risk is acceptable. By accepting risk, the management official is deciding to authorize the operation without additional mitigation at the present time. Each LOB and Staff Office to which this order is applicable must establish the levels of management that can accept safety risk based on the severity and likelihood. In order for the operation to be implemented, when the responsibility for managing the safety risk spans across more than one LOB or Staff Office, the residual safety risk must be accepted by the appropriate management official in each affected FAA organization. Accepting risk is a management decision. This policy does not compel a management official to accept risk, nor does it require FAA organizations to circumvent their existing risk acceptance criteria or safety standards.

b. Hazards may also be identified through the Safety Assurance functions used to monitor the aerospace system. In these situations, it is necessary to determine whether continued operation is acceptable (and for how long) while new safety risk controls are introduced. Each LOB and Staff Office to which this order is applicable must develop its own guidance and procedures for addressing existing high risk while working toward a mitigation plan to lower the safety risk. The guidance and procedures should include guidelines for managing and communicating elevated safety risk while developing a plan to reduce the safety risk. Table 2-1 (below) summarizes the management levels for safety risk acceptance.

**Table 2-1: Safety Risk Acceptance Criteria
for Issues or Changes That Cross LOBs/Staff Offices***

Initial Safety Risk Level	Safety Risk Acceptance Responsibility **
High Risk	Associate Administrators of LOBs; Assistant Administrators of Staff Offices; ATO Chief Operating Officer***
Medium Risk	The appropriate management officials within the stakeholder organizations who have the positional responsibility and authority for the issue or change being assessed****
Low Risk	Per LOB/Staff Office Guidance for Safety Risk Acceptance

* For Airworthiness Directives, acceptance of safety risk may be delegated in accordance with the current version of FAA Order 1100.154, *Delegations of Authority*.

** By accepting risk, the management official is deciding to authorize the operation without additional mitigation at the present time. Accepting risk is a management decision. This policy does not compel a management official to accept risk, nor does it require FAA organizations to circumvent their existing risk acceptance criteria or safety standards.

*** The ATO must comply with the current versions of FAA Order 1100.161, *Air Traffic Safety Oversight*, and FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, as well as the ATO SMS Manual. Per FAA Order JO 1000.37, the ATO Chief Operating Officer (COO) is informed of any existing hazards that are determined to be a high-risk hazard and any interim actions taken to mitigate the risk. The ATO COO either approves the interim action and accepts the associated risk or requires that the operation be stopped.

**** In general, risk acceptance decisions should be made at the lowest level possible in which the management officials accepting the risk have the responsibility and authority for the issue or change being assessed.

c. As described in Chapter 1, subparagraph 6c(1), 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 sufficient to mitigate the safety risk to a level that would be acceptable to the decision maker. Such limitations include the regulator's legal authority (which is established by statute and executive order), technological limitations, cost-benefit requirements for regulations, and the lack of cost-effective solutions. When this is the case, the FAA must document the analysis and any decisions made, apply the controls that it is able to, and establish a methodology to monitor the safety risk.

d. A methodology for monitoring and tracking the residual risk and assessing the safety risk against defined safety risk acceptance criteria should be defined for hazards with associated predicted safety risk that is medium or high. This methodology is documented in a monitoring plan, which is included in the documentation of the safety risk assessment. The monitoring plan describes who is responsible for tracking and monitoring and how it will be done. Specifically, the monitoring plan describes the tracking and monitoring activities, to include their frequency (how often they will be performed), their duration (how long the monitoring activities will be conducted), and the data necessary to evaluate the effectiveness of safety risk controls. In addition, the monitoring plan includes a description of the safety performance targets that will be used to assess the safety performance of existing controls and any newly implemented safety risk controls.

4. Safety Performance Monitoring and Hazard Tracking. Safety performance monitoring and hazard tracking include documenting safety risk controls, confirming the implementation and effectiveness of safety risk controls, and updating the residual risk levels, as appropriate.

a. Safety performance monitoring measures the effectiveness of existing and new safety risk controls, as well as provides information regarding the accuracy of the prediction of residual risk resulting from the risk analysis and assessment. Safety risk controls are determined to be effective when safety performance targets identified in monitoring plans are met. Safety performance monitoring is primarily accomplished through the Safety Assurance functions.

b. Hazard identification and tracking are foundational requirements for effective SRM. 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. LOBs and Staff Offices are responsible for identifying and tracking hazards within their purview. In addition, they are responsible for capturing and reporting the progress of identified ASL safety issues into HIRMT. While LOBs and Staff Offices can use their own tools to collect and maintain information regarding safety issues that are addressed wholly within their organization, if the safety issue meets the ASL criteria, the information must be entered into HIRMT. To become a user and be granted access to HIRMT, individuals must complete the HIRMT user training.⁸

c. A safety issue that meets one or more of the following criteria is considered an ASL issue and must be reported in and managed through HIRMT:

(1) The safety issue is tracked and managed by the FAA SMS Committee;

(2) The safety issue is present in the National Airspace System (NAS)⁹, its safety risk has not been accepted, and it is expected to have high risk (e.g., it is identified as a result of an accident or incident or it is assumed to have high risk but an assessment has not been completed);

(3) The safety issue has high risk and has a potentially systemic outcome (e.g., the outcome crosses LOBs or the outcome impacts an industry segment rather than an individual certificate holder); or

(4) Any safety issue that an FAA organization's management elects to track in HIRMT.¹⁰

d. The FAA SMS Committee monitors the reporting and closing of ASL safety issues in HIRMT. The OPR is responsible for entering the results of SRM and associated Safety Assurance efforts regarding ASL issues into HIRMT. For ASL safety issues that stay within an organization, the OPR will coordinate within their organization for safety risk acceptance, record that decision on behalf of their organization in HIRMT, and identify when an issue is closed. For cross-organizational

⁸ For more information regarding HIRMT and to obtain access to the tool, please refer to the HIRMT site on the FAA intranet at <https://hirmt.faa.gov> or contact the HIRMT Help Desk at 9-natl-hirmt-helpdesk@faa.gov.

⁹ Changes being processed through the NAS Change Proposal (NCP) may be considered to be present in the NAS if they are in the live test and evaluation phase.

¹⁰ The organization should consider the risk and visibility of a safety issue when determining if it should be entered into HIRMT.

issues, the OPR is responsible for coordinating safety risk acceptance decisions with the appropriate organizations, recording those decisions in HIRMT, and coordinating with the FAA SMS Committee to determine when the HIRMT record can be closed.

e. LOBs and Staff Offices that have a documented process/tool for capturing and managing safety issues that is comparable to the process in HIRMT, as determined by the FAA SMS Committee, are exempted from this requirement. In order for an LOB or Staff Office to receive an exemption from the requirement to use HIRMT, the organization must submit a formal request to the FAA SMS Committee for such an exemption. The request must include a description of the safety issue or type of safety issue for which the exemption is being requested, a detailed description of the process/tool that is or will be used to track the safety issue or type of safety issue, and documentation (e.g., policies, process/procedure documents, work instructions) that describes the tracking process/tool and its applicability.

5. Documenting Assessments and Decisions.

a. Safety risk acceptance decisions made as a result of the safety risk analysis must 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 safety risk is acceptable. The document should 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. If not using HIRMT, each LOB must identify the process and documentation used to document the findings and results of each step of the SRM process. The documentation should be written to be understood by a reviewer familiar with the discipline(s) relevant to the issue or change that was assessed.

c. The documentation should include:

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

(a) Name(s) and contact information;

(b) Organization(s); and

(c) Role of team member/individual in performing the analysis (e.g., area of expertise, organizational representative, or role such as a facilitator).

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

(a) Explanation of the trigger that resulted in undertaking the analysis;

(b) Statement reflecting the impact of the issue or change (e.g., industry segment and level of impact such as local, regional, and national);

- (c) Available data on related incidents or accidents;
 - (d) Existing safety risk controls;
 - (e) Pertinent interfaces and support systems required to maintain system function; and
 - (f) Reference to any other related analyses.
- (3) Identification of Hazards.
- (a) Description of the hazards and how they were identified; and
 - (b) Any additional existing controls related to the identified hazards that were not identified in the system analysis/description of the issues or change in paragraph 2 (above).
- (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) The 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; and
 - (d) Assumptions made and known limitations of the analysis, including margin of error when it was calculated.
- (5) Analysis of Proposed Safety Risk Controls.
- (a) Description of the safety risk controls that were considered;
 - (b) Description of proposed 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; and
 - (c) Residual safety risk.
 - 1) Description of any remaining safety risk, including risk created by the proposed safety risk controls and strategies employed to mitigate/control this new safety risk; and
 - 2) Description of how the hazards and their associated controls will be tracked and monitored against safety risk acceptance criteria.
- (6) Comments or Other Opinions. Description and source of the comments or other opinions from team members who want their input recorded (including the name and organization of the

commenter). If the comment or other opinion is in regard to the safety risk assessment, then it should include a risk matrix.

(7) Reviews (if applicable). Description of any peer reviews conducted.

(8) Safety Risk Acceptance and Approvals (if applicable).

(a) Name, position, and signature of management official(s)/executive(s) approving any safety risk controls and/or accepting the residual safety risk in accordance with Table 2-1, which is attached to the documentation by the OPR when acceptances and/or approvals are obtained; and

(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) Safety controls are currently in development that would sufficiently reduce safety risk; and
- 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 that will be taken to ensure safety 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 of the applicable FAA organizations (identified in Chapter 1, subparagraph 2).

2. Related Publications. This order was developed to be consistent with the latest versions of the following aviation safety documents that existed at the time the order was published:

- a. FAA Order 8000.369, *Safety Management System*
- b. FAA Order 1100.154, *Delegations of Authority*
- c. *AVP300-15-U.S. State Safety Program*
- d. FAA Order VS 8000.367, *Aviation Safety (AVS) Safety Management System Requirements*
- e. FAA Order 1100.161, *Air Traffic Safety Oversight*
- f. *Risk Analysis Specification* (Aircraft Certification Service)
- g. FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*
- h. *Air Traffic Organization, Safety Management System Manual*
- i. *Safety Risk Management Guidance for System Acquisitions (SRMGSA)*
- j. FAA Order 5200.11, *FAA Airports (ARP) Safety Management System*
- k. *FAA Office of Commercial Space Transportation Safety Management System (SMS) Manual*
- l. *Flight Safety Analysis Handbook* (Office of Commercial Space Transportation)
- m. *Safety Approval Guide for Applicants* (Office of Commercial Space Transportation)
- n. FAA Order NG 1000.44, *NextGen Safety Management System*
- o. *International Civil Aviation Organization Annexes 1, 6, 8, 11, 13, 14, 18, and 19*
- p. *ICAO Safety Management System Manual* (Document 9859)

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. Common Cause Failure – A failure that occurs when a single fault results in the corresponding failure of multiple system components or functions.

f. Control – See Safety Risk Control. The terms *Control*, *Mitigation*, and *Safety Risk Control* are used synonymously.

g. Effect – The real outcome that has occurred or the credible predicted outcome expected if the hazard exists in the defined system state.

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

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

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

k. Mitigation – A means to reduce or eliminate the effects of hazards. *See Safety Risk Control*. The terms *Control*, *Mitigation*, and *Safety Risk Control* are used synonymously.

l. Monitoring – Tracking and keeping information under systematic review.

m. Office of Primary Responsibility (OPR) – The organization that manages and tracks the issue or change through closure; responsibilities include leading and managing the safety risk assessment, identifying the appropriate management officials to accept safety risk and approve mitigations, coordinating any necessary approvals and safety risk acceptance decisions, and entering results and decisions into HIRMT, as required.

- n. Risk** – *See Safety Risk*. The terms *Risk* and *Safety Risk* are used synonymously.
- o. Risk Acceptance**. *See Safety Risk Acceptance*. The terms *Risk Acceptance* and *Safety Risk Acceptance* are used synonymously.
- p. Safety** – The state in which the risk of harm to persons or property damage is acceptable.
- q. 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.
- r. Safety Performance Target** – A measurable goal used to verify the predicted residual safety risk of a hazard's effect.
- s. Safety Risk** – The composite of predicted severity and likelihood of the potential effect of a hazard.

(1) Types of Safety Risk

- (a) Initial Risk – The predicted severity and likelihood of a hazard's effects or outcomes when it is first identified and assessed; includes the effects of preexisting safety risk controls in the current environment.
- (b) Residual Risk – The remaining predicted severity and likelihood that exists after all selected safety risk control techniques have been implemented.

(2) Levels of Safety Risk

- (a) High Risk – Severity and likelihood map to the red cells in the risk matrix (in Appendix C). This safety risk requires mitigation, tracking, and monitoring, and it can only be accepted at the highest level of management within LOBs and Staff Offices.
 - (b) Medium Risk – Severity and likelihood map to the yellow cells in the risk matrix (in Appendix C). This safety risk is acceptable without additional mitigation; however, tracking and monitoring are required.
 - (c) Low Risk – Severity and likelihood map to the green cells in the risk matrix (in Appendix C). This safety risk is acceptable without restriction or limitation; hazards are not required to be actively managed, but they must be documented and reported if a safety risk assessment has been performed.
- t. Safety Risk Acceptance** – The decision by the appropriate management official to authorize the operation without additional safety risk mitigation.
 - u. Safety Risk Analysis** – The first three steps of the SRM process (analyze the system, identify hazards, and analyze safety risk).

- v. Safety Risk Assessment** – The first four steps of the SRM process (analyze the system, identify hazards, analyze safety risk, and assess safety risk).
- w. Safety Risk Control** – A means to reduce or eliminate the effects of hazards. The terms *Control*, *Mitigation*, and *Safety Risk Control* are used synonymously.
- x. Safety Risk Management (SRM)** – A process within the SMS composed of describing the system; identifying the hazards; and analyzing, assessing, and controlling safety risk.
- y. Severity** – The consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm.
- z. Single Point Failure** – An element of a system or operation for which no backup (i.e., redundancy) exists. Single-pilot operations are an exception.
- aa. 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. **AGC** – Office of the Chief Counsel
- b. **AIR** – Aircraft Certification Service
- c. **ANG** – Office of the Next Generation Air Transportation System
- d. **AOV** – Air Traffic Safety Oversight Service
- e. **ARP** – Airports Organization
- f. **ASH** – Office of Security and Hazardous Materials Safety
- g. **ASL** – Aerospace System Level
- h. **AST** – Office of Commercial Space Transportation
- i. **ATO** – Air Traffic Organization
- j. **AVP** – Office of Accident Investigation and Prevention
- k. **AVS** – Aviation Safety Organization
- l. **COO** – Chief Operating Officer
- m. **FAA** – Federal Aviation Administration
- n. **FOIA** – Freedom of Information Act
- o. **HIRMT** – Hazard Identification, Risk Management & Tracking
- p. **ICAO** – International Civil Aviation Organization
- q. **LOB** – Line of Business
- r. **NAS** – National Airspace System
- s. **NCP** – NAS Change Proposal
- t. **OPR** – Office of Primary Responsibility
- u. **SMS** – Safety Management System
- v. **SRM** – Safety Risk Management
- w. **SRMGSA** – Safety Risk Management Guidance for System Acquisitions
- x. **SSP** – 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 LOB and Staff Office 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 LOB/Staff Office 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) that 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.

4. The severity and likelihood definitions in Table C-1, *Severity Definitions*; Table C-2, *Likelihood Definitions – Commercial Operations/Large Transport Category*; and Table C-3, *Likelihood Definitions – General Aviation Operations/Small Aircraft and Rotorcraft*, are used for cross-organizational safety risk assessments. Because of the differences in the segments of the system, there is a different likelihood definition table for commercial operations (Table C-2) and general aviation operations (Table C-3); however, the same severity definitions (Table C-1) are used for both. The assessment team determines the appropriate definitions to use based on the issue/change being assessed. When the issue or change being assessed might include both commercial and general aviation, the issue or change should be parsed into separate items to allow targeted assessments and enable the appropriate definitions to be used. If the issue or change cannot be parsed into separate items, the more stringent definitions should be used. The assessment team may determine that it needs to develop definitions and accompanying rationale that better fit the issue or change being analyzed (and not use Tables C-1, C-2, and/or C-3). For instance, some segments of the aerospace system do not have the number of operations necessary to fit into the quantitative likelihood definitions described in Tables C-2 and C-3. When developing specific likelihood definitions, consideration should be given to the number of vehicles, number of operations, or size of the system and ensure that they align to the qualitative definitions listed in Tables C-2 and C-3.

Table C-2: Likelihood Definitions – Commercial Operations/Large Transport Category

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 10 times per year
Probable B	Expected to occur often	Expected to occur between one and 10 times per year
Remote C	Expected to occur infrequently	Expected to occur one time every 1 to 3 years
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 3 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than once every 10 years

Table C-3: Likelihood Definitions – General Aviation Operations/Small Aircraft and Rotorcraft

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 100 times per year (or more than approximately 10 times a month)
Probable B	Expected to occur often	Expected to occur between 10 and 100 times per year (or approximately 1-10 times a month)
Remote C	Expected to occur infrequently	Expected to occur one time every 1 month to 1 year
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 1 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than one time every 10 years

5. A risk matrix is a graphical means of depicting safety risk. 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. The risk matrices in Figure C-1, *Risk Matrix – Commercial Operations/Large Transport Category*, and Figure C-2, *Risk Matrix – General Aviation Operations/Small Aircraft and Rotorcraft*, are used in the Assess Safety Risk step of SRM. Again, because of the differences in the segments of the system, there is a different risk matrix for commercial operations and general aviation operations. The risk matrix in Figure C-1 should be used for assessing the safety risk of commercial operations, including large transport category aircraft. The risk matrix in Figure C-2 should be used for assessing the safety risk of general aviation operations, including small aircraft and rotorcraft.

When the issue or change being assessed might include both commercial and general aviation, the issue or change should be parsed into separate items to allow targeted assessments and enable the appropriate risk matrix to be used.

Severity Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	[Green]	[Yellow]	[Red]	[Red]	[Red]
Probable B	[Green]	[Yellow]	[Red]	[Red]	[Red]
Remote C	[Green]	[Yellow]	[Yellow]	[Red]	[Red]
Extremely Remote D	[Green]	[Green]	[Yellow]	[Yellow]	[Red]
Extremely Improbable E	[Green]	[Green]	[Green]	[Yellow]	[Red] * [Yellow]

High Risk [Red]

Medium Risk [Yellow]

Low Risk [Green]

* High Risk with Single Point and/or Common Cause Failures

Figure C-1: Risk Matrix – Commercial Operations/Large Transport Category

Severity Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	[Green]	[Yellow]	[Red]	[Red]	[Red]
Probable B	[Green]	[Yellow]	[Yellow]	[Red]	[Red]
Remote C	[Green]	[Green]	[Yellow]	[Yellow]	[Red]
Extremely Remote D	[Green]	[Green]	[Green]	[Yellow]	[Red] * [Yellow]
Extremely Improbable E	[Green]	[Green]	[Green]	[Green]	[Yellow]

High Risk [Red]

Medium Risk [Yellow]

Low Risk [Green]

* High Risk with Single Point and/or Common Cause Failures

Figure C-2: Risk Matrix – General Aviation Operations/Small Aircraft and Rotorcraft

6. 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 LOBs and/or Staff Offices and with management. The risk matrix is a tool that facilitates communication regarding safety risk among FAA organizations through the graphical illustration of safety risk analysis and assessment results. Using the risk matrix across LOBs and/or Staff Offices 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 an LOB or Staff Office. Therefore, if a hazard, its associated safety risk, and safety risk controls stay within an LOB or Staff Office, the FAA organization may use its existing safety risk assessment methodology. In most cases, the organization does not have to translate its assessment into the risk matrix included in this order. However, when a hazard meets the ASL criteria described in Chapter 2, subparagraph 4c, information regarding the hazard must be input into HIRMT, and the hazard must be plotted onto one of the matrices depicted in Figure C-1 or Figure C-2 (based on the type of operation) to facilitate communication and coordination.

When the team conducting the assessment is comprised of members from LOBs and Staff Offices that use different risk matrices, the team uses the risk matrix in this policy, unless all stakeholder FAA organizations agree to use a different method or tool. For cases in which controlling safety risk is outside the authority of the FAA (as described in Chapter 2, subparagraph 3c of this order), 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 safety risk.

7. The safety risk levels used in the process are defined below.

a. High Risk – Severity and likelihood map to the red cells in the risk matrix (in Appendix C). This safety risk requires mitigation, tracking, and monitoring, and it can only be accepted at the highest level of management within LOBs and Staff Offices (see Table 2-1). In the operational environment, it is understood that high risk may exist in the short term. Some organizations have established short-term risk acceptance guidelines contained in formal LOB processes that establish management approval of high short-term risk. When this is the case (except for ASL issues), those processes are followed while new safety risk controls are developed and implemented and do not require additional approvals described in Table 2-1.

b. Medium Risk – Severity and likelihood map to the yellow cells in the risk matrix (in Appendix C). This safety risk is acceptable without additional mitigation; however, tracking and monitoring are required. It is desirable to achieve the lowest practicable risk levels (factoring in the principles of appropriate resource management), thus mitigation of medium risk is recommended but not required.

c. Low Risk – Severity and likelihood map to the green cells in the risk matrix (in Appendix C). This safety risk is acceptable without restriction or limitation; hazards are not required to be actively managed, but they must be documented and reported if a safety risk assessment has been performed.

8. 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 high; if the box is yellow, the safety risk associated with the hazard is acceptable with monitoring; 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 safety risk is plotted. Plotting the prediction of the residual safety risk illustrates the impact of the safety risk controls on the initial safety risk and shows the decision maker whether the safety risk associated with the hazard will be mitigated to an acceptable level.
- 9.** Ranking the safety risk associated with the identified hazards helps the team and decision maker prioritize the development and implementation of mitigations.

Appendix D. Disclosure for FAA Personnel to Participate on SRM Teams

The FAA's participation on an SRM Team established and led by entities outside the FAA is voluntary, and FAA personnel can leave SRM Team meetings any time they choose. The SRM Team lead is also free to ask FAA personnel to leave an SRM Team meeting any time they deem appropriate.

The FAA has the responsibility and authority to conduct regulatory oversight in the aerospace system. FAA participation on the SRM Team in no way affects the FAA's ability to pursue any compliance action or enforcement actions that it deems appropriate and to use information obtained in connection with its membership on the team in such actions.

FAA employees' participation on the SRM Team does not constitute FAA's endorsement of the findings of the SRM Team or any actions that result from the assessment conducted by the team. Further, when an FAA employee participating on an SRM Team provides an opinion or adds to the team's discussion or knowledge base in any way, that employee is not providing an official FAA position on the topic. For an official FAA position or interpretation, a formal request must be submitted to the FAA.

The undersigned acknowledges that he/she has received this document and understands the scope of the FAA employee's participation on the SRM Team as set forth above.

Authorized Representative (signature)

Date

Authorized Representative (print)