**FOREWORD**

The fundamental mission of our company is to ensure the safe operations in our location/region. Thanks to its employees, our company operates the safest, most efficient (our company type, such as airline, AMO, flight school, etc.) in the world.

Our company uses the Safety Management System (SMS) to develop an intensive, proactive, and systematic focus on assuring safety. The SMS constitutes operating principles supporting our company in objectively examining the safety of our operations.

This document is the result of a company-wide effort, and reflects current international best practices and lessons learned. It marks an important next step toward a mature and integrated SMS in our company. Therefore, it is important that all company personnel work diligently to uphold and follow the procedures and guidance in this SMS Manual to manage safety risk and help promote a positive safety culture in our company.

This SMS manual is a living, breathing document and is subject to change.

Joe Brown

CEO

This SMS Manual is a template. You are required to make changes based on your unique organizational differences.

Items suggested for Search and review:

* Director of Quality
* Director of Safety
* 1.3.3 Safety Policy
* 1.3.4 Non-punitive reporting policy
* 1.3.5 Fatigue Risk Management Policy
* 3.6.4 Risk Acceptance Decision-Making Authority
* Review list in section "3.2.1 When to Perform a Safety Analysis"
* Review list in section "3.2.2.3 Examples of Changes Unlikely to Require a Safety Analysis"
* Safety Risk Management committee
* SRM committee
* Review “Safety and technical training department.” You may call this the QA department, or Safety & Quality Dept. You may need to change this name in the SMS Manual to align with your structure
* Review Org Chart in Section 1.4.1 and replace
* Review list of system changesthat will require a safety analysis in 3.2.1
* Review 6.1 MOC signatures
* Review Table 3.5 Likelihood of Effect
* Review 7.2.3 regarding ASAP program

Contents

[1.1 Overview 3](#_Toc515887218)

[1.1.1 About the SMS Manual 3](#_Toc515887219)

[1.1.2 Establishment and Continuous Support of our Company SMS 3](#_Toc515887220)

[1.1.3 SMS Continuous Improvement 3](#_Toc515887221)

[1.1.3.1 Measuring Safety Performance 3](#_Toc515887222)

[1.1.4 SMS Benefits 3](#_Toc515887223)

[1.2 Four Components of SMS 3](#_Toc515887224)

[1.2.1 SMS Components 3](#_Toc515887225)

[1.2.2 Safety Culture and Promotion: Valuing Safety in Our Company 3](#_Toc515887226)

[1.3 SMS Policy 6](#_Toc515887227)

[1.3.1 SMS Policy Derivations 6](#_Toc515887228)

[1.3.2 Policy Compliance with SMS 6](#_Toc515887229)

[1.3.3 Safety Policy Statement 7](#_Toc515887230)

[1.3.4 Non-punitive Reporting Policy 7](#_Toc515887231)

[1.3.5 Fatigue Risk Management Policy 9](#_Toc515887232)

[1.4 Roles and Responsibilities 11](#_Toc515887233)

[1.4.1 Company Safety Organization 11](#_Toc515887234)

[1.4.2 Personnel Duties and Responsibilities 12](#_Toc515887235)

[1.5 Safety Communications 14](#_Toc515887236)

[1.5.1 Safety Reporting 14](#_Toc515887237)

[1.5.1.1 Employee Confidential Reporting System 15](#_Toc515887238)

[1.5.2 Safety Communication Tools 18](#_Toc515887239)

[1.6 Safety Management Goals and Objectives 19](#_Toc515887240)

[1.6.1 How to Develop Goals 20](#_Toc515887241)

[1.6.2 Safety Objectives and Safety Performance Goals 22](#_Toc515887242)

[1.6.3 Annual Safety Reports 22](#_Toc515887243)

[2.1 Safety Risk Management (SRM) and Safety Assurance (SA) 23](#_Toc515887244)

[2.1.1 Introduction to Managing System Safety 23](#_Toc515887245)

[2.1.2 Safety Assessment Using the Tenets of SRM and SA 23](#_Toc515887246)

[2.1.3 SRM: Proactive and Reactive Hazard and Risk Reduction 24](#_Toc515887247)

[2.1.4 Safety Assurance (SA): Identifying and Closing Safety Gaps 25](#_Toc515887248)

[2.2 Identifying and Addressing System Vulnerabilities 26](#_Toc515887249)

[2.2.1 System Gaps and Hazard Defenses 26](#_Toc515887250)

[2.2.2 The Human Element’s Effect on Safety 27](#_Toc515887251)

[2.2.3 Closing Gaps Using SRM and SA Principles and Processes 28](#_Toc515887252)

[2.2.4 Safety Order of Precedence 29](#_Toc515887253)

[2.2.5 Hierarchy of Control 30](#_Toc515887254)

[3.1 Safety Risk Management (SRM) Overview 30](#_Toc515887255)

[3.1.1 Overview of the SRM Process 30](#_Toc515887256)

[3.1.2 SRM Safety Analysis Phases 32](#_Toc515887257)

[3.2 Scope of the SRM Process 32](#_Toc515887258)

[3.2.1 When to Perform a Safety Analysis 33](#_Toc515887259)

[3.2.2 When a Safety Analysis May Not Be Required 34](#_Toc515887260)

[3.3 SRM Phase 1: Describe System 36](#_Toc515887261)

[3.3.1 Overview 36](#_Toc515887262)

[3.3.2 Bounding and Scoping Safety Analyses 36](#_Toc515887263)

[3.3.3 Defining the System / System Change 37](#_Toc515887264)

[3.4 SRM Phase 2: Identify Hazards 41](#_Toc515887265)

[3.4.1 Overview 41](#_Toc515887266)

[3.4.2 Potential Sources of Hazards 41](#_Toc515887267)

[3.4.3 Elements of Hazard Identification 43](#_Toc515887268)

[3.4.4 Causes and System State Defined 45](#_Toc515887269)

[3.5 SRM Phase 3: Analyze Risk 45](#_Toc515887270)

[3.5.1 Overview 45](#_Toc515887271)

[3.5.2 Controls 46](#_Toc515887272)

[3.5.3 Determining a Credible Hazard Consequence or Effect 48](#_Toc515887273)

[3.5.4 Defining Risk 48](#_Toc515887274)

[3.6 SRM Phase 4: Assess Risk 52](#_Toc515887275)

[3.6.1 Overview 52](#_Toc515887276)

[3.6.2 Risk Levels and Definitions 52](#_Toc515887277)

[3.6.3 Plotting Risk for Each Hazard, Reported Issue or Audit Finding 53](#_Toc515887278)

[3.6.4 Risk Acceptance Decision-Making Authority - Reactive 54](#_Toc515887279)

[3.7 SRM Phase 5: Treat Risk 55](#_Toc515887280)

[3.7.1 Overview 55](#_Toc515887281)

[3.7.2 Risk Management Strategies 55](#_Toc515887282)

[3.7.3 Documenting Safety Requirements 57](#_Toc515887283)

[3.7.4 Determining Predicted Residual Risk 57](#_Toc515887284)

[4.1 Developing Safety Performance Targets 58](#_Toc515887285)

[4.2 Developing the Monitoring Plan 58](#_Toc515887286)

[4.2.1 Monitoring Activities 58](#_Toc515887287)

[4.2.2 Frequency and Duration of Monitoring 60](#_Toc515887288)

[4.3 Post-SRM Monitoring 60](#_Toc515887289)

[4.3.1 Monitoring and Current Risk 60](#_Toc515887290)

[4.3.2 Predicted Residual Risk Is Not Met 61](#_Toc515887291)

[4.3.3 Predicted Residual Risk Is Met 61](#_Toc515887292)

[4.3.4 Residual Risk 61](#_Toc515887293)

[4.3.5 Monitoring and Tracking of Changes Added to System 62](#_Toc515887294)

[5.1 Safety Analysis Overview 63](#_Toc515887295)

[5.1.1 Safety Analysis Process Flow 63](#_Toc515887296)

[5.2 Preparing a Safety Analysis 63](#_Toc515887297)

[5.2.1 Planning and Initial Decision-Making 63](#_Toc515887298)

[5.2.2 Preparing for In-Depth Safety Analyses 64](#_Toc515887299)

[5.3 Performing a Safety Analysis 68](#_Toc515887300)

[5.3.1 First Day of the SRM Committee 68](#_Toc515887301)

[5.3.2 Administering the SRM Committee Meeting 69](#_Toc515887302)

[5.3.3 Factors that Jeopardize Safety Assessment Results 69](#_Toc515887303)

[5.3.4 SRM Committee Deliberations 69](#_Toc515887304)

[5.4 Documenting a Safety Analysis 69](#_Toc515887305)

[5.4.1 MOC SRM Documents 69](#_Toc515887306)

[5.4.2 MOC – Management of Change (MOC) 70](#_Toc515887307)

[5.4.3 Completing the MOC SRM Document 70](#_Toc515887308)

[5.4.4 Implementation Dates in PHAT and Issue Manager 74](#_Toc515887309)

[5.5 Special SRM Efforts/Considerations 74](#_Toc515887310)

[5.5.1 Deactivation, Removal, or Decommissioning of Equipment 74](#_Toc515887311)

[5.5.2 Emergency Modifications 75](#_Toc515887312)

[5.5.3 Existing High-Risk Hazards 75](#_Toc515887313)

[6.1 Risk Acceptance and Approval and Overview 76](#_Toc515887314)

[6.2 Scope of Changes 79](#_Toc515887315)

[6.2.1 Local Implementation of System-Wide Changes 80](#_Toc515887316)

[6.3 Approving Safety Requirements 80](#_Toc515887317)

[6.3.1 Appropriate Signatories 80](#_Toc515887318)

[6.3.2 Endorsing Implementation of Safety Requirements 80](#_Toc515887319)

[6.4 Risk Acceptance 81](#_Toc515887320)

[6.4.1 Authority to Accept Safety Risk 82](#_Toc515887321)

[6.4.2 Risk Acceptance Outside of our Company 82](#_Toc515887322)

[6.5 MOC SRM Document Approval 82](#_Toc515887323)

[6.5.1 Department MOC SRM Documentation Approval 83](#_Toc515887324)

[6.5.2 Safety and Technical Training Department Review and Approval 83](#_Toc515887325)

[6.5.3 Coordination of MOC SRM Documentation 84](#_Toc515887326)

[7.1 Audit and Assessment Programs 84](#_Toc515887327)

[7.1.1 Overview 84](#_Toc515887328)

[7.1.2 Difference between Facility Audits and Assessments 84](#_Toc515887329)

[7.1.3 Independent Assessments 84](#_Toc515887330)

[7.2 Safety Data Reporting, Tracking, and Analysis 85](#_Toc515887331)

[7.2.1 Purpose of Safety Data Collection and Evaluation 85](#_Toc515887332)

[7.2.2 Safety and Training Department’s Role in Safety Data Collection and Evaluation 86](#_Toc515887333)

[7.2.3 Safety Data Collection and Reporting Processes 86](#_Toc515887334)

[7.3 Safety Incident and Accident Reporting and Analysis 86](#_Toc515887335)

[7.3.1 Delegating Risk Management Tasks 87](#_Toc515887336)

[7.3.2 Corrective and Preventive Action Management 92](#_Toc515887337)

[7.3.3 Closing Reported Issues, Findings and Setting Review Dates 93](#_Toc515887338)

[7.3.4 Closing Feedback Loop with Reported Issue Submitter 93](#_Toc515887339)

[7.3.5 Safety Committee Review of Hazard Reports 94](#_Toc515887340)

[7.3.6 Validating Reported Issues and Audit Findings 94](#_Toc515887341)

[7.4 Reported Safety Data about Serviceability of Equipment, Systems, and Facilities 94](#_Toc515887342)

[7.5 Voluntary Data Reporting 95](#_Toc515887343)

[8.1 Safety Data Gathering and Review Overview 95](#_Toc515887344)

[9.1 Part 5 FAA Required SMS Processes and Procedures 100](#_Toc515887345)

[9.1.1 Identify Hazards 100](#_Toc515887346)

[9.1.2 Analyze Safety Risk 100](#_Toc515887347)

[9.1.3 Conducting Risk Assessments 100](#_Toc515887348)

[9.1.4 Developing Safety Risk Controls 100](#_Toc515887349)

[9.1.5 Acquiring Data to Monitor Operational Processes 101](#_Toc515887350)

[9.1.6 Acquiring Data to Monitor Operational Environments 101](#_Toc515887351)

[9.1.7 Auditing Operational Processes and Systems 101](#_Toc515887352)

[9.1.8 Evaluating SMS and Operational Processes 101](#_Toc515887353)

[9.1.9 Investigation of Incidents and Accidents 101](#_Toc515887354)

[9.1.10 Investigating Potential Non-compliance Reports 102](#_Toc515887355)

[9.1.11 Confidential Employee Reporting System 102](#_Toc515887356)

[9.1.12 Analyzing Safety Data 102](#_Toc515887357)

[9.1.13 Correcting Safety Performance Deficiencies 102](#_Toc515887358)

[10.1 Definitions 102](#_Toc515887359)

[11.1 Acronyms 109](#_Toc515887360)

## 1.1 Overview

### 1.1.1 About the SMS Manual

Our Safety Management System (SMS) is a formalized and proactive approach to system safety. It directly supports ICAO requirements and the mission of our civil aviation authority (CAA), which is “to provide the safest, most efficient aerospace system in the world.” Our **SMS** is an integrated collection of principles, policies, processes, procedures, and programs used to identify, analyze, assess, manage, and monitor safety risk while providing our company’s services.

Our SMS Manual informs employees and contractors about the goal of our company SMS, describes the interrelationship among the four components of the SMS, and instructs readers on the process of identifying safety hazards and mitigating risk in our operations. Use this document to carry out the safety mission of the CAA and the required SMS elements.

### 1.1.2 Establishment and Continuous Support of our Company SMS

**Safety**, the principal consideration of all our company activities, is defined as the state in which the risk of harm to persons or property damage is acceptable. Managing and ensuring the safety of operations using SMS has long been a focus of aviation service providers worldwide, with the International Civil Aviation Organization having provided the guiding principles and the mandate for member organizations to have an SMS. Our company’s SMS efforts support our CAA safety mission, which emphasizes continuous improvement of safety and the integration of safety management activities within our organization.

### 1.1.3 SMS Continuous Improvement

SMS is the framework that our company uses to measure and help ensure the safety of its operations. In an evolving environment, it is necessary to continuously seek improvement in our processes and policies supporting our business efforts and, by extension, support the SMS.

Our company and external organizations conduct audits and assessments to measure and determine our compliance with policies and procedures used to manage safety. By assessing SMS maturity, our company is able to identify gaps in SMS performance, opportunities for improvement, and areas in which to focus new policy development.

Our company uses a variety of tools to measure continuous improvement. These tools include our SMS database that collects, collates and presents SMS data for management review. Modules in the SMS database (see section 8.1) to measure and monitor continuous improvement include:

* Executive Dashboard;
* Gap Analysis;
* Risk Impact Trending Charts;
* CPA Manager;
* Risk Analysis Charts;
* Risk Exposure;
* KPI Trend Monitor;
* Continuous Improvement; and
* Goals and Objectives.

### 1.1.3.1 Measuring Safety Performance

As part of the effort to support our CAA SMS initiatives, our company uses the SMS database’s Rolling KPI Dashboard as a measure of its safety performance. The Rolling KPI Dashboard provides a 12-month rolling rate that compares the number of important safety issues (or events) within our company. This module allows our company to easily identify performance issues by configuring red and yellow visual alerts based on types of events.

Safety issues are identified, assessed and classified as part of the integrated Safety Risk Management (SRM) and Safety Assurance (SA) processes, which considers contributing factors when assessing severity and frequency of the issue(s) that have been reported, or for identified safety hazards.

Through the integrated SRM and SA process, reported issues and audit findings replace the long-standing measures of safety performance in our company, allowing relationships to be drawn between events and potential causes. From performance of individual departments up to company-wide operations, integrated SRM and SA processes help focus our company’s safety initiatives on significant causes, issues, and hazards that necessitate remedial action, thus, advancing risk-based decision-making initiatives.

### 1.1.4 SMS Benefits

Processes and tools supporting SMS help:

* Provide a common framework to proactively and reactively identify and address safety hazards and risks associated with our company’s equipment, operations, and procedures;
* Encourage company stakeholders to participate in solving the safety challenges of an increasingly complex operating environment;
* Reduce isolated analysis and decision-making using integrated safety management principles;
* Improve accountability for safety through defined managerial roles and responsibilities and SRM processes;
* Integrate Safety Assurance processes enabling our company to effectively monitor and measure safety performance;
* Promote a continuous cycle of assessing, correcting/mitigating, and monitoring our company’s level of safety;
* Foster a positive safety culture that can help improve system safety; and
* Measure the performance and support the improvement of the SMS.

## 1.2 Four Components of SMS

### 1.2.1 SMS Components

The four components of the Safety Management System (SMS) combine to create a systemic approach to managing and ensuring safety. These components are:

* **Safety Policy:** The documented organizational policy that defines management’s commitment, responsibility, and accountability for safety. Safety Policy identifies and assigns responsibilities to key safety personnel.
* **Safety Risk Management (SRM):** A process within the SMS composed of describing the system; identifying the hazards; and analyzing, assessing, and controlling risk. SRM includes processes to define strategies for monitoring the safety risk of our company. SRM complements Safety Assurance.
* **Safety Assurance:** A set of processes within the SMS that verify that the organization meets or exceeds its safety performance objectives and that function systematically to determine the effectiveness of safety risk controls through the collection, analysis, and assessment of information.
* **Safety Promotion:** The communication and distribution of information to improve the safety culture and the development and implementation of programs and/or processes that support the integration and continuous improvement of the SMS within our company. Safety Promotion allows our company to share and provide evidence of successes and lessons learned.

### 1.2.2 Safety Culture and Promotion: Valuing Safety in Our Company

#### 1.2.2.1 Overview of Safety Culture, Safety Assurance, and SRM

**Safety culture** is defined as the way safety is perceived and valued in an organization. It represents the priority given to safety at all levels in the organization and reflects the real commitment to safety. Our company uses its SMS to promote a positive safety culture through policies that align safety goals with organizational standards, training, voluntary reporting, safety communications and best practices.

A strong safety culture helps ensure that personnel are trained and competent to perform their duties and that continual training and updates on safety progress are provided. Promoting strong safety values means that all our employees share lessons learned from investigations and experiences, both internally and from other organizations. All employees have access to desensitized safety issues in the SMS database’s *General Issue Viewer*, where they can investigate types of issues or hazards our company has identified. We also allow all employees to further their knowledge by providing access to the SMS database’s *Lessons Learned Library*.

Safety Risk Management (SRM) and Safety Assurance (SA) are the performance-oriented components and results of the SMS, but programs and work contributing to the Safety Promotion component are vital to achieving positive safety outcomes throughout our company.

The tenets of Safety Promotion are used to foster a positive safety culture in which our employees understand why safety is important and how they affect it, providing a sense of purpose to safety efforts. Each employee must consider the potential effect their decisions may have on safety and is responsible for understanding the significance of his or her job as it relates to safety.

SMS training identifies the importance of the SMS and how each employee and contractor fits into the mission of using the SMS to improve safety in our company. Each employee is required to participate in SMS training, which is documented in the SMS database’s *SMS Induction* module. We use self-paced computer-based training (CBT) to provide initial SMS training. Our SMS CBT is integrated in the SMS database and is required for all employees with access to the SMS database.

Open communication is critical to a positive safety culture. Our company communicates safety goals and objectives to all operational personnel to improve the way safety is perceived, valued, and prioritized. Company safety goals and objectives are visible to all employees via the SMS database’s *Goals and Objectives* module.

In an organization with a strong safety culture, individuals and groups take responsibility for safety by communicating safety concerns and striving to learn, adapt, and modify individual and organizational behavior based on lessons learned. Safety promotion communications are disseminated to employees by various tools in the SMS database, including:

* Safety Newsletters;
* Message Board;
* Safety Surveys;
* Lessons Learned Library; and
* Training Article Library.

#### 1.2.2.2 Safety Programs and Initiatives

Our company maintains a positive safety culture using programs and initiatives such as:

* **Recurrent Training:** Collaboratively-developed instruction for employees, designed to maintain and update previously learned skills while promoting a positive safety culture. Our company’s SMS database uses the *Training Article Library* to supplement and document recurrent training activities.
* **Top 5:** High-priority factors that contribute to the risk in our company. The Top 5 is determined based on data obtained from SRM and SA processes and using our company’s SMS database to log and report unsafe occurrences. The SMS database’s *Executive Dashboard* is instrumental in aggregating and communicating risk to all employees.
* **Fatigue Risk Management:** A group that provides operational fatigue risk expertise, guidance, and support to our company’s policy in developing fatigue reduction strategies and policy recommendations to mitigate and manage operational fatigue risks in our company.
* **Partnership for Safety:** A joint effort that encourages employees to become actively engaged in identifying local hazards and developing safety solutions before incidents occur. Supporting this program is the SMS database Hazard Reporting module to proactively alert management of potential hazards and compliance issues.
* **Mandatory and Voluntary Safety Reporting Program:** A confidential reporting system for employees and other stakeholders to identify and report safety and operational concerns.
* **Lessons Learned:** Lessons learned are used to improve company processes, address deficiencies proactively, and empower employees to play a direct role in company safety by providing valuable safety information. Company lessons learned are available in our SMS database’s *Lessons Learned Library*.
* **Safety Newsletters:** Our company safety newsletter is a safety promotion communication tool of our safety department. We use safety newsletters to disseminate information to our stakeholders, which include employees, managers, suppliers, vendors and contractors. Our safety newsletter helps form a bond of community and keeps stakeholders informed of planned safety training and activities. We also use our safety newsletter to break down those strong barriers to change. Historical safety newsletters can be reviewed in our SMS database's *Safety Newsletters* module.

## 1.3 SMS Policy

### 1.3.1 SMS Policy Derivations

Our SMS is supported by numerous levels of policy and requirements.

#### 1.3.1.1 ICAO SMS Policy

Our company derives its high-level SMS policy from International Civil Aviation Organization (ICAO) policy. [ICAO Annex 19, *Safety Management*, provides standards and recommended practices](http://www.icao.int/safety/SafetyManagement/Pages/Annex-19,-1st-Edition---Executive-summary.aspx) for safety management for member states and air traffic service providers. Additionally, [ICAO Document 9859, *Safety Management Manual*, provides guidance for the development and](http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf) implementation of the SMS. [ICAO Document 9859](http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf) also provides guidance for safety programs in accordance with the international standards and recommended practices contained in Annex 19.

#### 1.3.1.2 FAA SMS Policy

The current version of [FAA Advisory Circular 120-92B, Safety Management Systems for Aviation Service Providers, describes the](http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1029147) essential aspects of an SMS and provides implementation guidance. This document is designed to create a minimum SMS standard that each organization can follow to implement an SMS.

The current version of [FAA Order 8040.4, Safety Risk Management Policy, provides risk](http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1019950) management policy to follow when hazards, risks, and associated safety analyses affect multiple areas of operations. Our company considers and, when necessary, uses the provisions in this order when coordinating safety assessments with other organizations. Our Director of Safety will function as our company liaison to interface with outside organizations. Within our company, the Director of Safety will adjudicate conflicts and discrepancies among corporate units.

### 1.3.2 Policy Compliance with SMS

As our company’s SMS matures, the tenets of the SMS components are integrated into new and existing company policy. For any policy or procedure to be considered compliant with the SMS, it must incorporate safety measures and SMS requirements to help manage safety.

#### 1.3.2.1 Safety Policy Requirements

Our company's safety policy must include at least the following:

* Our company's safety objectives (or reference to their location);
* CEO's commitment to fulfill the organization’s safety objectives;
* A clear statement about providing the necessary resources for SMS implementation;
* Reference to our safety reporting policy that defines requirements for employee reporting of safety hazards, incidents, accidents or issues.
* Reference to our company policy defining unacceptable behavior and conditions for disciplinary action.
* Reference to our company's emergency response plan that provides for the safe transition from normal to emergency operations according to section 1.3.2.1 Emergency Response Plan.

Our company safety policy must be:

* Signed by the accountable executive;
* Annually reviewed by the accountable executive to ensure it remains relevant and appropriate to our operations; and
* Documented and visible to all employees by accessing company Policies and Procedures in our SMS database

#### 1.3.2.2 Emergency Response Plan Requirements

Where emergency response procedures are necessary, our company must maintain and the accountable executive must approve as part of the safety policy, the emergency response plan that addresses:

* Delegation of emergency authority throughout our company;
* Assignment of employee responsibilities during the emergency; and
* Coordination of emergency response plans with the emergency response plans of other organizations we must interface with during the provision of its services.

### 1.3.3 Safety Policy Statement

Our company, in partnership with its employees will conduct business in a manner that ensures the health and safety of its employees, customers, and the general public while meeting its obligations under all applicable regulations.

Our Company provides a hazard reporting database called SMS Pro, where employees can confidentially report hazards, and where safety or compliance hazards receive Risk Analysis and Risk Management by the safety team and operational department heads.

Our company remains committed to fulfilling our company safety goals and objectives. Company safety goals and objectives are made available to all employees in our company SMS database under the menu item: “Policy >> Goals and Objectives.” At a minimum, all employees are required to review company safety goals and objectives during their initial and recurrent SMS training.

Our company has established a Safety Management System that provides a systematic approach to safety in the following areas:

* Safety Management Plan
* Documentation
* Risk Management
* Training
* Quality Assurance
* Emergency Response

The established Safety Management System will allow us to meet our company safety goals:

* Commitment to communication
* Promotion of Safe Practices
* Continuous Improvement

All employees must commit to the principle that “*Safety is everyone’s responsibility*.”

### 1.3.4 Non-punitive Reporting Policy

At our company, our objective is to cultivate and foster a generative safety culture in which employees and customers are comfortable and encouraged to bring safety concerns to the attention of management.

**Non-punitive Reporting Policy Statement**

No person will be penalized or retaliated against for bringing safety issues to the attention of management.

* Safe operations are our company’s most important commitment. To ensure this commitment, it is imperative that we have uninhibited reporting of all incidents and occurrences that compromise the safety of our operations.
* We ask that each employee accept the responsibility to communicate any information that may affect the integrity of flight safety. Employees must be assured that this communication will never result in reprisal, thus allowing a timely, uninhibited flow of information to occur
* All employees are advised that our company will not initiate disciplinary action against an employee who discloses an incident or occurrence involving flight safety. This policy cannot apply to criminal, international or regulatory infractions
* Our company has developed safety reports to be used by all employees for reporting information concerning flight safety. They are designed to protect the identity of the employee who provides information. These forms are readily available in your work area.
* We urge all employees to use this program to help our company continue its leadership in providing our customers and employees with the highest level of flight safety.

Any employee who feels they are being subjected to discipline or discrimination may request a review of the situation/circumstances with the Director of Safety and their immediate supervisor, as applicable.

#### 1.3.4.1 Exceptions to Non-punitive Reporting Policy

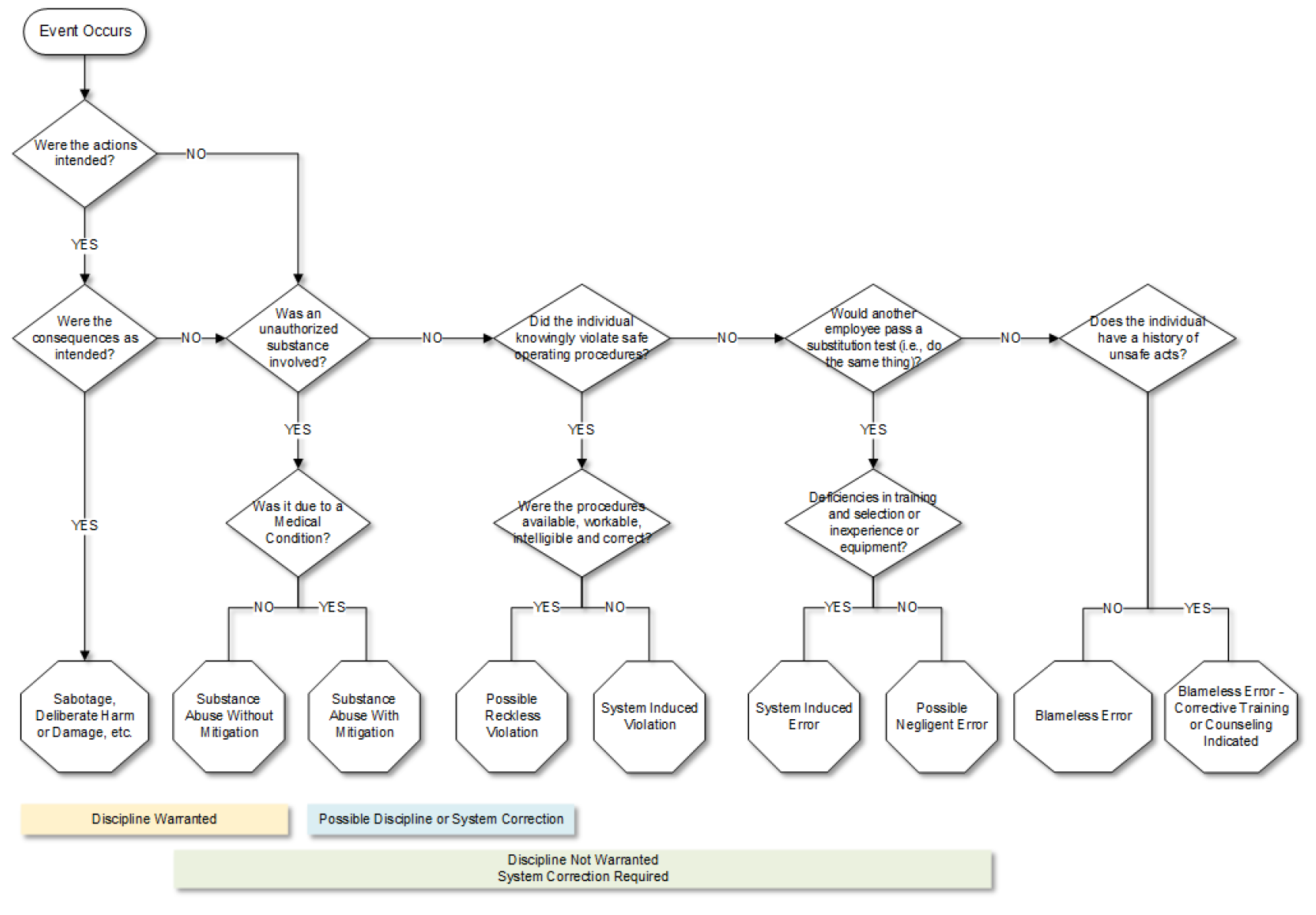
As outlined in our company's Non-punitive Reporting Policy, no employee shall be disciplined or discriminated against, in any way, for reporting a health and safety concern or hazard to company management. It is only through teamwork that unhealthy or unsafe conditions or practices can be rectified. Our main objective is to enhance safety, and we realize unreported faulty conditions cannot be rectified unless employees trust the process and have assurance against retaliation.

The success of our SMS and accident prevention program depends upon the support and commitment of everyone. However, in the event the reported incident was a result of reckless or willful behavior, discipline may be warranted.

Cases that nullify the Non-punitive Reporting Policy include:

* **Reckless Violation**: Is more culpable than negligence. It involves a person taking a conscious unjustified risk, knowing that there is a risk that harm would probably result from the conduct, and foreseeing the harm, he or she nevertheless took the risk. It differs from negligence (where negligence is the failure to recognize a risk that should have been recognized), while recklessness is a conscious disregard of an obvious risk.
* **Intentional "Willful" Violation**: When a person knew or foresaw the result of the action but went ahead and did it anyway.

Any incident that may be considered for discipline will be investigated thoroughly, and the results reviewed by Management before any disciplinary action is taken. The flowchart shown in Fig. 1.1 displays a decision tree to assist in deciding the culpability of an unsafe act. The assumption is that the actions under review have contributed to an occurrence or to a serious incident.



**Figure 1.1 Non-punitive Issue Verification Model**

The purpose of the above flowchart helps management determine human/negligent error vs. willful or reckless behavior.

### 1.3.5 Fatigue Risk Management Policy

#### 1.3.5.1 Purpose and Intended Outcomes

The purpose of this policy is to establish the requirements for managing fatigue. It is intended that this policy will reduce the risk of fatigue-related injuries and incidents in the workplace.

#### 1.3.5.2 Scope and Coverage

This policy applies to all staff, especially those whose work involves shift work, extended hours and on-call arrangements.

#### 1.3.5.3 Fatigue Risk Management Policy Statement

Our Company is committed to providing and maintaining safe systems of work for all its workers, including those whose work involves shifts work, extended hours or on-call arrangements.

Our Company’s operations are sometimes undertaken outside ordinary working hours. Activities such as [insert examples] often involve shift work, extended hours and on-call arrangements. These working arrangements may contribute to fatigue if not managed appropriately. Fatigue can be caused by both work and non-work-related factors. Non-work factors include

* family responsibilities,
* social activities,
* health issues—such as sleep disorders,
* study commitments and
* sporting commitments.

Work factors include

* shift work (especially night shift), and
* working extended hours.

While everyone doesn’t respond to fatigue in the same way, fatigue can cause

* reduced concentration,
* impaired coordination,
* compromised judgement and
* slower reaction times.

These effects ultimately increase the risk of incidents and injury.

#### 1.3.5.4 Responsibilities

Managers and workers of our Company have a responsibility to ensure that fatigue does not impact the safety, health and well-being of themselves and others.

**Managers and supervisors are responsible for:**

* Applying risk management in consultation with staff and in accordance with the fatigue risk management system.
* Ensuring systems of work that minimize the risk of fatigue—for example,
  + reasonable rosters,
  + reasonable overtime practices and
  + adequate recuperation between shifts.
* Providing opportunities for workers to obtain adequate rest from work.
* Monitoring workloads, work patterns and rostering arrangements to ensure workers are not placed at risk from fatigue
* Consulting with workers when introducing shift work or new rostering systems.
* Providing information, instruction and training about risks to health, safety or welfare of workers involved with shift work, extended hours and on-call arrangements.
* Ensuring workers performing shift work are properly supervised and that tasks are undertaken safely.
* Referring workers with non-work fatigue related issues to the employee assistance program.

**Workers are responsible for:**

* Participating in risk management processes.
* Using time off from work to recuperate to be fit and able for the next shift.
* Participating in education and training to gain an understanding of fatigue.
* Avoiding behaviors and practices that contribute to fatigue and which could place themselves and others at risk, for example,
  + secondary employment or
  + not using time off work to recuperate.
* Recognizing signs of fatigue that could place the health, safety and well-being of themselves or others at risk and reporting this to their manager or supervisor.

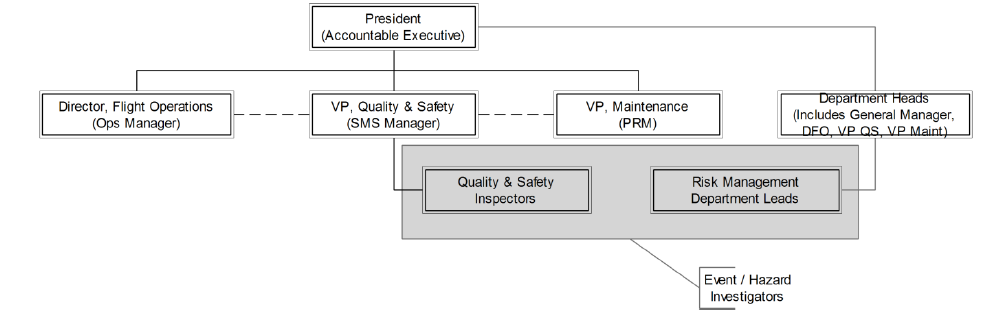
#### 1.3.5.5 Results from Breaches of Policy

Breaches of this policy and/or any of its associated procedures may result in disciplinary action being initiated in accordance with our Company’s Discipline Policy.

## 1.4 Roles and Responsibilities

### 1.4.1 Company Safety Organization

The Company Safety Organization is shown below. Senior leaders are responsible for establishing and managing safety management programs within the department(s) under their control that are consistent with corporate and regulatory requirements. The Director of Safety coordinates development, operation and quality control of our company's Safety Management System.



### 1.4.2 Personnel Duties and Responsibilities

#### 1.4.2.1 Accountable Executive

Our Accountable Executive is the person who has control of the financial and human resources that are necessary for the activities and operations authorized under our certificate. The accountable executive maintains final authority over operations authorized to be conducted under our company's certificate(s); therefore, he retains ultimate responsibility for company safety performance.

Our company’s Safety Management System (SMS) encompasses the Flight Operations, Maintenance, Cargo and Customer Service Agent departments as well as all corporate departments. Our company therefore requires the Accountable Executive to maintain financial and executive control over all company operations.

The Accountable Executive has executive responsibility for our company's safety performance and for effective operation of the company SMS.

The Accountable Executive shall ensure:

* appropriate organizational and financial resources are available to support SMS programs;
* SMS is properly implemented and performing in all areas of our organization;
* all members of the Executive and Management teams are aware of applicable SMS requirements as identified in this document and CAA regulations;
* all members of the Executive and Management teams actively promote and support SMS programs;
* an annual review is conducted our company's safety performance and direct necessary actions to address substandard safety performance. and
* all members of the Executive and Management teams maintain effective interdepartmental communication in support of the company SMS.

The Accountable Executive may not delegate his responsibilities to any person, but he may delegate certain SMS duties to the VP, Quality & Safety.

The Accountable Executive is accountable to the civil aviation authority and all employees in carrying out these responsibilities.

#### 1.4.2.2 Director of Safety (SMS Manager)

The Director of Safety is responsible for the performance of the Safety Management System, the Quality Assurance Program and the Quality and Safety Inspectors. If resources are required, a request will be made to the Director of Safety to ensure support is provided for the development and maintenance of the Quality Assurance Program and all audit activities contained therein. A direct line of communication will be maintained with the Accountable Executive. All audit results will be communicated to the Accountable Executive and applicable department heads.

The person assigned the role of Director of Safety shall:

* Establish and maintain the SMS Program to ensure the timely collection of information related to hazards, incidents and accidents that may adversely affect safety;
* Identify hazards and carry out risk management analyses of those hazards;
* Investigate, analyze and identify the cause or probable cause of all hazards, incidents and accidents identified under the safety management system;
* Establish and maintain a safety data system, to monitor and analyze trends in hazards, incidents and accidents;
* Monitor and evaluate the results of corrective actions with respect to hazards, incidents and accidents;
* Monitor the concerns of the civil aviation industry in respect of safety and their perceived effect on our company;
* Establish the SMS training program and determine the adequacy of the training required for applicable staff;
* Approve all policy and procedural changes to the SMS and QA programs;
* Establish and maintain the Quality Assurance (QA) Program
* Report the hazards, incidents and accidents identified under the SMS or as a result of an audit to upper management and the Accountable Executive;
* Monitor the effectiveness of safety risk controls;
* Facilitate hazard identification and safety risk analysis;
* Ensure safety promotion activities are performed throughout the company.

#### 1.4.2.3 Department Heads (Vice Presidents, Directors, Managers)

All Department heads are responsible for SMS duties within their respective areas including, but not limited to:

* Developing and maintaining departmental procedures, processes, and control of applicable manuals in their department;
* Ensuring compliance with regulations and managing regulatory issues within their department;
* Create a hazard/event report for any accident or incident that have occurred or have been reported to them;
* Attend and participate in applicable safety management meetings;
* Foster and promote the organizations Safety Management System in their respective area;
* Identify and assess hazards through the risk management process;
* Develop and implement corrective, preventative or mitigating actions as required;
* Initiate proactive analysis and safety projects with the Director of Safety to address changes to processes, systems or regulatory requirements to ensure adequate safety standards are maintained;
* Ensure personnel under their authority complete required Safety Management training;
* Advising the accountable executive on the performance of the SMS in their department and on any need for improvement;
* Assuring the effectiveness of safety risk controls in their area of operation;
* Participate in or conduct hazard identification and safety risk assessments;
* Participate in or conduct accident, incident, and/or hazard investigations; and
* Actively promote Quality and Safety in their department

#### 1.4.2.4 All Employees

Everyone at our company is responsible for ensuring the safety of our employees, passengers and assets. All employees shall report any incidents, hazards, near misses and work-related illness to their supervisor immediately. Employees have a duty and responsibility to follow our organization’s processes and procedures.

Additionally, all employees shall:

* Be aware of our company’s safety policies, as well as the processes, procedures, and tools relevant to their responsibilities.
* Know how the confidential employee reporting system works;
* Follow directions to use safety materials, equipment, devices and/or clothing (Personal Protective Equipment – PPE), and standard operating procedures (SOPs);
* Comply with instructions from the organization, or from a Health and Safety Officer;
* Report injuries, accidents, anything or circumstance that is hazardous or that is likely to become hazardous; and
* Cooperate with Health and Safety committees.

#### 1.4.2.5 Safety Management Committee

The Safety Management Committee is a chaired by the Director of Safety or his delegate, whose purpose is to establish overall safety policies, make decisions and suggestions where risk assessments or corrective actions have not been accepted by department heads, and provide direction on the ongoing development and maintenance of the Safety Management System.

The Safety Management Committee includes the following members:

* Accountable Executive
* Operations Manager (Director, Flight Operations)
* Person Responsible for Maintenance
* General Manager
* SMS Manager (Director of Safety)

#### 1.4.2.6 Management Review Committee

The purpose of the Management Review Committee is to review the company’s safety management system to ensure its continuing adequacy and effectiveness as well as review the company’s safety performance and achievements.

The Management Review Committee will consist of the following Management Personnel:

* Accountable Executive
* Operations Manager (Director, Flight Operations)
* Person Responsible for Maintenance
* General Manager
* SMS Manager (Director of Safety)

## 1.5 Safety Communications

### 1.5.1 Safety Reporting

A key and vital component of an effective and dynamic SMS is communication. Without effective two-way communication, the success of any safety program is jeopardized.

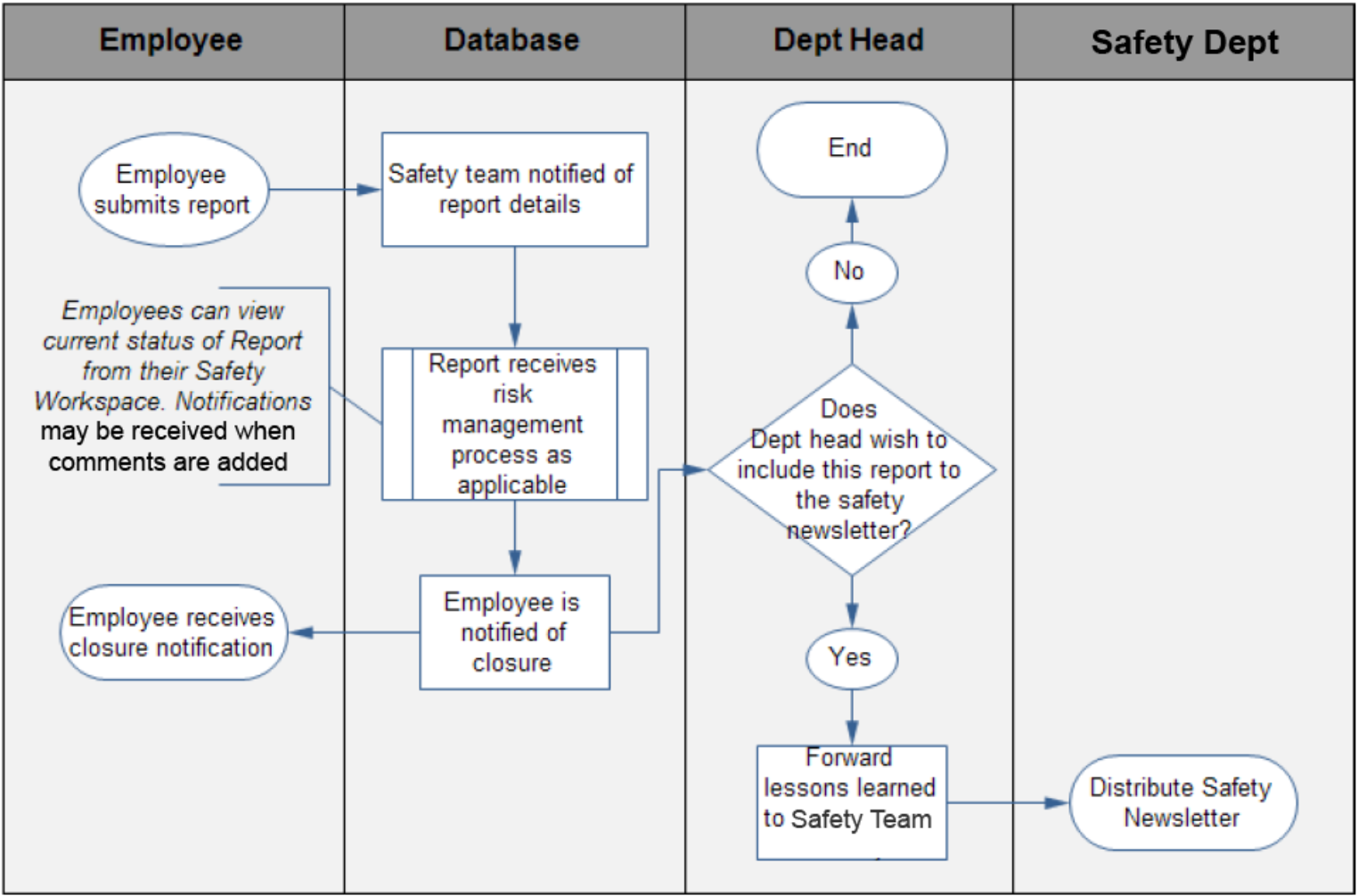
Employees who complete and submit safety reports shall be advised via their email address (when provided by the reporter) that the report has been received.

Employees submitting reported issues can elect to receive immediate feedback on the investigation results and corrective actions where applied. When submitted reports fall outside the bounds of SMS, employees submitting irrelevant reports are notified by email the reason the report is not relevant by a safety team member. These reasons are documented in the SMS database, as well as the date the employee was notified and by which safety team member.

Additional feedback from investigations, audits and other safety analyses may be provided in any of the following ways:

* Changes to procedures
* Addressed in training
* Department or corporate memos and/or bulletins
* Safety update newsletters
* Direct contact with stakeholders
* Lessons Learned in safety newsletters
* Lessons Learned Library module in SMS database

Figure 1.5.1 shows example of the feedback loop and how safety communications may be initiated.



**Figure 1.5.1 Safety Reporting Communication Feedback Loop**

### 1.5.1.1 Employee Confidential Reporting System

Our company uses an online SMS database to capture:

* Identified hazards by employees;
* Incidents;
* Accidents; and
* Potential non-compliance issues.

Employees with user accounts in the SMS database will login to the SMS database and report issues using the *Hazard Reporting* module. Other stakeholders without user accounts in the SMS database can submit issues using the SMS database’s *Public Issue Reporting* module or by email. Reported issues submitted by email are addressed to [safety@myCompany.com](mailto:safety@myCompany.com) and configured in the SMS database. The SMS database alerts the safety team when new email reports enter the system.

Our company's confidential reporting system is non-punitive, so there will be no disciplinary action for reporting a hazard or incident that was not purposefully or negligently committed. These reported issues are used to collect and classify information to identify trends that help determine whether additional controls merit implementation to prevent future hazards, incidents, occurrences, or accidents.

At our company, a hazard is anything that, in the eyes of the employee or customer, threatens the safety of people of resources. To this end, a Reported Issue shall be submitted when any situation, practice, procedure, or process is observed which is either:

* A recognized safety concern;
* Considered unusual from an operational or procedural standpoint;
* Considered deficient from a safety standpoint;
* A potential or actualized regulatory noncompliance;
* Possesses a foreseeable potential for injury/illness to persons or damage or loss of property if not addressed in a timely manner.

When reporting issues in the SMS database, adding your name is optional to maintain anonymity, however, it is encouraged that your name and contact information is provided in the event that further information is required to mitigate hazard effects.

Another option when submitting reported issues is to remain confidential. Utilizing this feature ensures that the reporters identity and the issue itself will not be disclosed to anyone else other than the assigned Safety Manager, investigator or investigation team member unless required by law. When reporters choose to have their reported issue remain confidential, they need to click the "I wish to remain confidential" checkbox when filling out the report to alert the safety team of their desire to keep the report within the confines of the safety team.

Reported issues should be concise and should accurately and thoroughly describe the hazard, incident, accident or irregularity. When applicable, reports should include the submitter's recommendation(s) for corrective action and any actions taken to immediately treat the situation.

In circumstances where the perceived hazard possesses an immediate potential for injury/illness to persons or damage/loss of property, management shall be notified immediately by the most expeditious means possible for the purpose of determining appropriate action to prevent such injury/illness or damage/loss.

Any incident involving company personnel, customers or property must be reported via the online reporting tool in the SMS database or by email. This list includes, but is not limited to:

* Injury or illness to any individual(s) which occurs in a company workplace or resulting from contact with company equipment and results in either hospitalization or treatment by a medical professional
* Any damage to company equipment or other property damage involving company personnel or property
* Any deviation from established laws, regulations, limitations, procedures, or practices by company personnel while performing employment related duties
* An occurrence which requires submission of a report to the NTSB
* Unintentional or uncontrolled release of any hazardous chemical in any company workplace
* Unintentional fire or indication of fire in company workplace or property
* Any physical incapacitation of a crewmember while performing duties which affects or could affect the ability employees to perform assigned duties
* Any time an emergency is declared during operations
* Unplanned operation in close proximity to another aircraft which creates a collision hazard
* Excursion from a runway or taxiway hard surface
* Encounter with severe turbulence or any icing accumulation
* Foreign Object Damage
* Bird or wildlife strike
* Operation of an aircraft outside of designed operating limitations

Upon receipt of the Reported Issue notification, the safety team will initiate a standard investigation in the SMS database to determine the validity of the report as well as to gain additional information concerning the report's subject matter. Any hazardous situations or equipment shall be either placarded or removed from service until the hazardous situation is corrected. The submitter, if identified, as well as all affected employees will be advised of the result of the investigation.

Once a report is validated, the safety team shall:

* Draft a preliminary risk statement;
* Conduct an initial risk assessment;
* Confirm a Targeted Closure Date (due date for reported issue);
* Assign the reported issue to related company department;
* Identify and notify the Department Head with risk acceptance authority for the area of affected operations; and
* Classify the issue according to type of issue and associated hazards from Hazard Risk Register if applicable.

The contents of the reported issue, investigation results, and recommendations for corrective/preventive action are always available through the SMS database to the responsible manager and the person who reported the issue.

#### 1.5.1.2 Issue Reporting Process

* Event Occurs/Hazard Detected
* Fill out report online or sends email to SMS database
* Report is automatically e-mailed to safety team
* Initial Risk Assessment using risk matrix described in Section 3.6
* Confirm the Targeted Closure Date (desired due date per policy)
* Assign responsible manager
* Classify the issue
* Determination of depth of the investigation (required or not required)
* Develop corrective action plan (CPAs)
* Review report at safety committee meeting
* Feedback to Reporter (if external to SMS database)
* Take Action/Alert employees of change
* Communicate Lessons Learned via Lessons Learned Library in SMS database
* Validation/review date entered into database for monitoring

### 1.5.2 Safety Communication Tools

There are numerous communication tools available to provide information about safety management processes, achievements, activities, investigations and quality management programs.

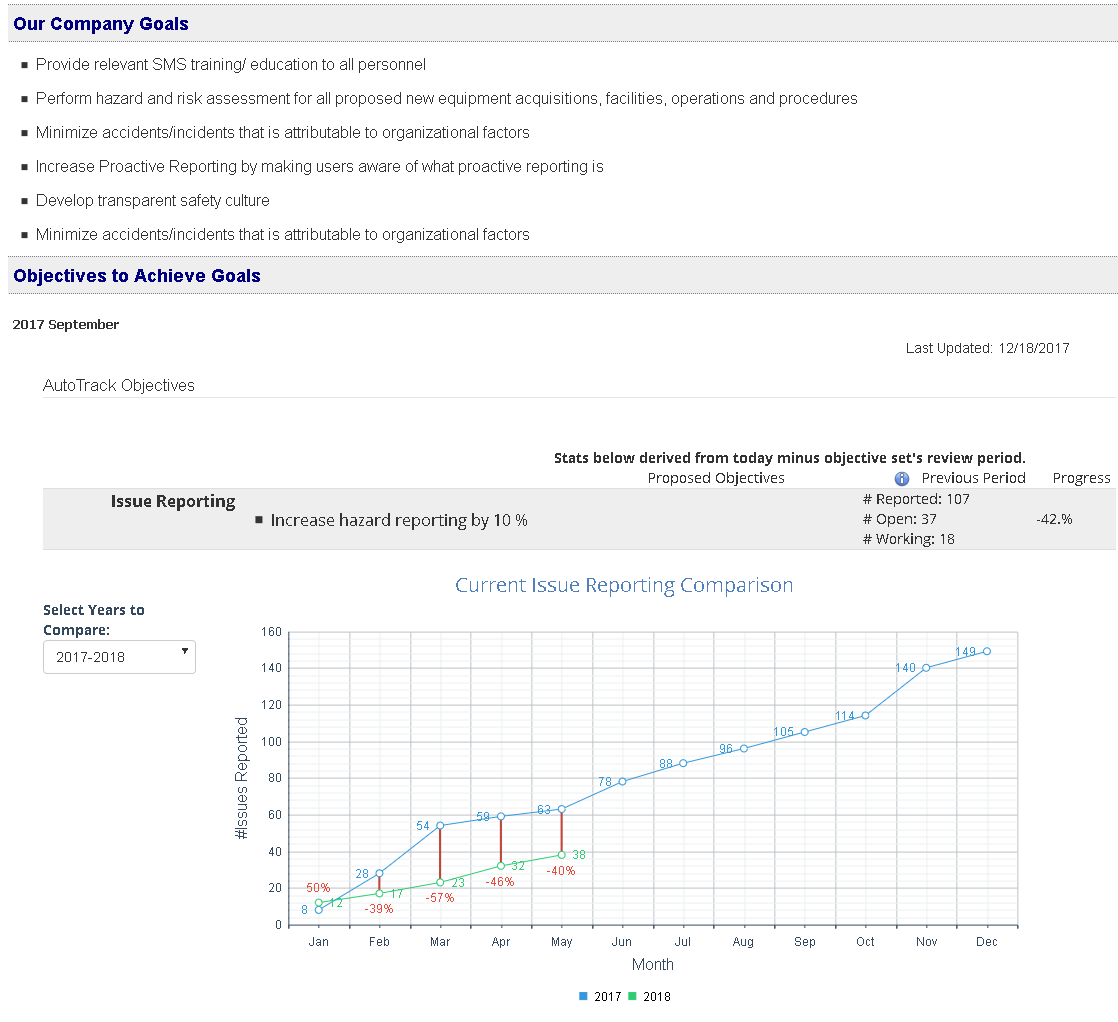
Below are the options available; each shall be utilized or not depending on the appropriateness of the vehicle and the message.

* Electronic Message Board – in SMS database
* Safety Meetings – Documented in Meeting Manager in SMS database
* Email – from SMS database’s Issue Manager and Message Board
* Safety Newsletters – from SMS database
* Paper copy Bulletins and Memos
* Posters
* Verbal communication
* Company hazard reporting database (SMS Pro)
* Safety Surveys (managed in SMS database)
* Training Article Library – in SMS database
* Lessons Learned Library – in SMS database
* General Issue Viewer – in SMS database

## 1.6 Safety Management Goals and Objectives

Current Safety Management Goals can be found in the company’s SMS database under Policy >> Goals and Objectives. Goals and objectives are reviewed quarterly by the safety committee. During the first quarter of each year, the Director of Safety will facilitate the review of the past year’s safety goals and objectives and determine goals and objectives for the current year.

Below in Figure 1.6 is an example of Safety Goals & Objectives from the SMS database:



**Figure 1.6 Example of Goals and Objectives in SMS Database**

### 1.6.1 How to Develop Goals

**Set Specific Goals**

An organizational safety goal must be clear and well defined. Vague or generalized goals are unhelpful because they don't provide sufficient direction. Remember, we need safety goals to show the way. Make it easy for us get where we want to go by defining precisely where we want to end up.

**Set Measurable Goals**

Include precise amounts, dates, and so on in organizational safety goals so we can measure our degree of success. If our goal is simply defined as "To improve hazard reporting" how will we know when we have been successful? In one month's time if we have a 1 percent increase or in two years' time when we have a 10 percent increase? Without a way to measure our success, we won’t know we have actually achieved our safety goal.

**Set Attainable Goals**

Make sure that it's possible to achieve our set safety goals. If we set a goal that we have no hope of achieving, we will only demoralize employees and erode their confidence in the SMS process.

However, resist the urge to set safety goals that are too easy or meaningless. Accomplishing a goal that doesn't require hard work or is irrelevant to our company’s mission can be anticlimactic at best and can also make us fear setting future goals that carry a risk of non-achievement. The best safety goals require us to "raise the bar" and they bring the greatest personal satisfaction when achieved.

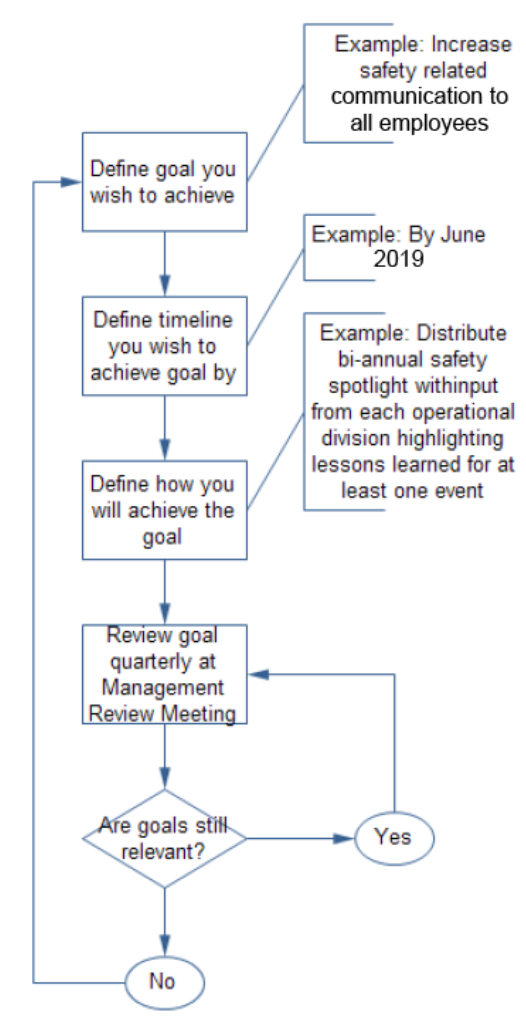
**Set Relevant Goals**

Goals should be relevant to the direction our organization must take. By keeping safety goals aligned with our SMS’ purpose, we'll develop the focus we need to achieve something meaningful. Avoid setting widely scattered and inconsistent goals.

**Set Time-Bound Goals**

Our safety goals must have a deadline or time-period. Again, this helps indicate when we have reached our target.

Figure 1.6.1 below shows a process to aid in setting and reviewing organizational safety goals.



**Figure 1.6.1 Setting Organizational Safety Goals**

### 1.6.2 Safety Objectives and Safety Performance Goals

Each operational Department Head shall be responsible for setting annual safety goals based on hazards and risks identified within the department(s) or division(s) under their control. In the SMS database, division-specific hazard registers identify the most significant risks to each department's operations and shall guide determination of annual department safety goals.

The following tools in our company’s SMS database should also be reviewed to identify hazards and risks to focus goals and objectives:

* Executive Dashboard;
* KPI Trend Monitor;
* Hazard Risk Register;
* Continuous Improvement Charts;
* Goals & Objectives;
* Risk Analysis Charts;
* Risk Impact Trending Charts;
* Rolling KPI Dashboard

For each safety goal, create objectives that are measurable, time-based and are consistent with the Safety Policy. Safety goals, objectives and key performance indicators (KPIs) shall be included in annual safety reports.

When specific safety goals or objectives are not met within an annual planning cycle, an explanation shall be included in the department's safety report. Safety goals or objectives that are not met shall only be included in the next planning cycle if department planning procedures indicate they need to be carried forward. For example, a safety goal that is not met may not be included in the next cycle due to changes in procedures or equipment or because other safety goals take priority.

Safety goals may be

* specific performance targets,
* safety management processes or controls, or
* positive year-over-year safety trends.

Timelines and performance measurement criteria shall be specified for each safety objective.

### 1.6.3 Annual Safety Reports

Department Heads of operational areas shall be responsible for submitting a safety report for the department(s) under their control. These departmental safety reports are used to create the annual company safety report.

Safety reports shall include a summary of each department's safety performance and identify specific safety goals, objectives and key performance indicators (KPIs). Safety reports shall also include any trends in elevated risk exposure identified. The *Risk Exposure* module in the SMS database can be used to identify risk exposure trends.

## 2.1 Safety Risk Management (SRM) and Safety Assurance (SA)

### 2.1.1 Introduction to Managing System Safety

As operational procedures and equipment (i.e., hardware and software) evolve, their interaction and interdependency across departments within our company must be addressed. In a system that relies upon external agencies, the discovery of a safety hazard and reduction of its risk often falls within the purview of multiple organizations.

The effects of safety hazards and associated risk reduction methods across multiple organizations, domains, and implementation timelines must be properly understood to achieve the highest practical level of safety.

Safety risk deemed acceptable for an individual corporate unit may lead to unintentional safety risk in another if a safety assessment is not conducted with a “system of systems” philosophy.

As new operations, policies and procedures are tested and implemented, safety risk assessments must account for their potential safety impact on existing/legacy tools and procedures and vice versa.

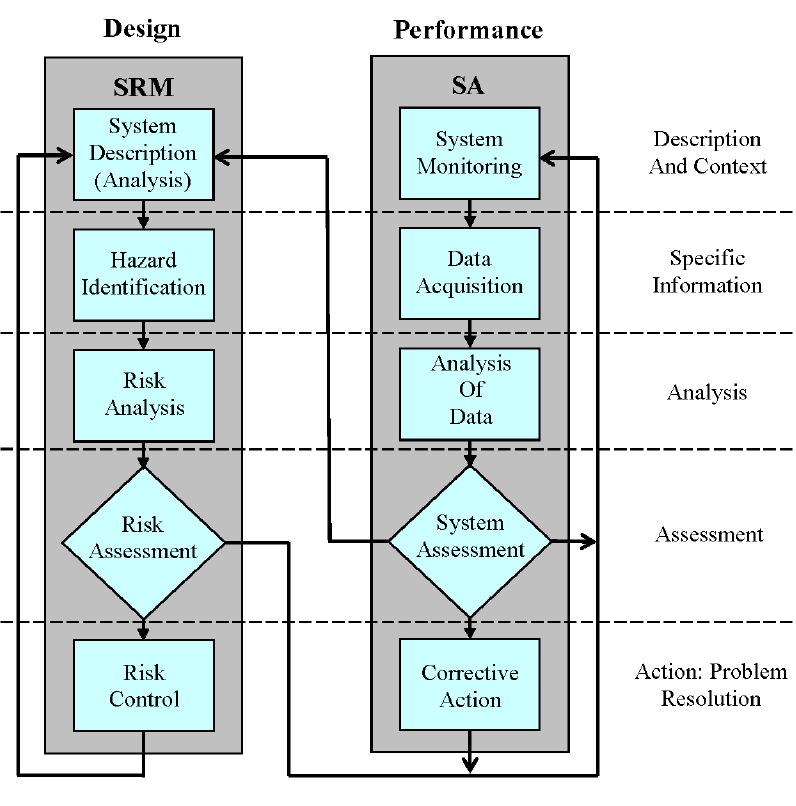
Sharing safety data and conducting cooperative analyses using an integrated safety management approach helps identify and resolve issues requiring the consideration of multiple disciplines. The goal of an integrated approach to safety management is to eliminate gaps in safety analyses by assessing and monitoring equipment, operations, and procedures.

### 2.1.2 Safety Assessment Using the Tenets of SRM and SA

In acknowledging the complexity of the aviation transportation system and its various system interdependencies, our company uses the systematic processes and tenets of Safety Risk Management (SRM) and Safety Assurance (SA) to identify and address safety hazards and risks across our operations.

The remainder of this chapter discusses foundational concepts and practices used to identify and address safety issues and consider potential ramifications in an integrated way. It will describe at a high level the underlying causes of safety hazards and the means by which our company manages safety risk.

The SRM process provides the framework to monitor an operational change after it has been implemented, using SA functions like assessments and employee hazard reporting to determine whether controls and/or recommended safety requirements are performing as intended/designed. Refer to Figure 2.2 for a depiction of the relationship between SRM and SA.



**Figure 2.2: SRM / SA Process Flow**

### 2.1.3 SRM: Proactive and Reactive Hazard and Risk Reduction

SRM is a formalized approach to integrated system safety. It both informs decision-makers about the potential hazards, safety risks, and ways to reduce risk associated with a particular change-request proposal and identifies ways to mitigate existing hazards in our operations. The methodology is applied to all company equipment, operations, and procedures to identify safety hazards and address risk.

It is important to understand that though our company uses SRM as a formal safety and risk assessment process, its philosophy is easily understood outside of the technical realm of aviation. For example, a person performs SRM each time he or she crosses the street. The individual identifies hazards (cars passing), analyzes and assesses the risk (potential to be struck and severity if he or she is), and explores ways to reduce the perceived risk (looking both ways for traffic and/or heeding pedestrian signals) to an acceptable level before proceeding.

It is necessary to make the approach to managing safety risk into a formalized, objective process. This helps ensure the effective management and reduction of a safety hazard’s risks. SRM provides a means to:

* Identify potential hazards and analyze and assess operational safety risk;
* Define safety requirements to reduce risk to an acceptable level;
* Identify safety performance targets, the measurable goals used to verify the predicted residual risk of a hazard; and
* Create a plan that an organization can use to determine if expected risk levels are met and maintained.

Refer to Section 3 for further guidance and the process for using SRM to perform a safety analysis.

### 2.1.4 Safety Assurance (SA): Identifying and Closing Safety Gaps

SRM alone does not assure the safety of the services our company provides; equally important are the efforts performed under the umbrella of SA. Safety Assurance builds on SRM efforts by:

* collecting and assessing data to monitor compliance,
* assess the performance of safety measures, and
* identify safety trends.

The Safety Assurance component of SMS encompasses all of our company processes and programs. These processes and programs can lead to the discovery of previously unidentified existing hazards and/or risk controls that are outdated or no longer effective. SA provides the means to determine whether equipment, operations, and procedures—and changes to them—meet or exceed acceptable safety levels.

#### 2.1.4.1 Audits and Assessments

To continuously improve the safety of its operations and procedures, our company conducts audits and assessments to determine whether they are performing as expected. Management also uses audit and assessment techniques to test, validate, and verify safety data obtained and produced by various entities and organizations. Furthermore, audits and assessments identify causes and correlations that can improve the understanding of safety performance.

Audits and assessments verify suspected positive and negative safety trends identified through analysis. In the event that a safety hazard is identified through an audit and/or assessment, SRM is used to identify potential and/or known risk reduction methods. In this sense, SA and SRM complement each other by providing a continuous loop of hazard identification and risk reduction methods.

A simplistic description of SRM and SA inter-relationships is: SRM is the design of the system, while SA monitors and validates the design.

Audits and assessments may be scheduled or unscheduled formal reviews, examinations, or verifications of activities, controls, operations, and systems. The scope of safety audit and assessment activities can vary. An audit or assessment can either focus on a single procedure or piece of equipment, or it can broadly examine multiple elements of a system.

Assessments fall into two categories:

* **Operational:** An assessment to address the effectiveness and efficiency of the organization. The objective of an operational assessment is to determine the organization’s ability to achieve its goals and accomplish its mission.
* **Compliance:** An audit that evaluates conformance to established criteria, processes, and work practices. The objective of a compliance audit is to determine whether employees and processes have followed established policies and procedures.

Our company uses both operational assessments and compliance audits. Using the above described methodologies, our company assesses safety performance through:

* Proactive evaluation of facilities, equipment, documentation, and procedures (e.g., internal assessments);
* Proactive evaluation of operational performance, thus verifying the fulfillment of operations’ safety responsibilities (e.g., periodic competency checks in the form of Quality Control, operational skills assessments, and system safety reviews); and
* Periodic evaluations to verify a system’s performance in control and reduction of safety risks (e.g., internal and external audits and/or assessments).

#### 2.1.4.2 Quality Assurance and Quality Control

Responsibilities for assessing trends and non-compliance fall under the jurisdiction of the Director of Quality, as well as managing procedures for identifying and correcting performance deficiencies.

Continuous improvement of the safety of our company can occur only when we remain vigilant in monitoring the performance of our operations and the implemented corrective actions. Refer to Section 7 for more information about our company programs that fit within the Safety Assurance component of the SMS.

## 2.2 Identifying and Addressing System Vulnerabilities

Before assessing safety risk or auditing safety performance, it is important to acknowledge the potential origins of safety hazards in our operations. Daily operations in an ever-changing environment can present varying hazards and levels of safety risk.

Given the complex interplay of human, material, and environmental factors in our operations, the complete elimination of all hazards and safety risk is unachievable. Even in organizations with excellent training programs and a strong safety culture, mechanical and electronic equipment will fail, software will function in an unintended manner, and human operators will make errors.

### 2.2.1 System Gaps and Hazard Defenses

#### 2.2.1.1 Overview and Causes of System Gaps

Developing a safe procedure, hardware, or software system requires that the procedure/system contain multiple defenses, ensuring that no single event or sequence of events results in an incident or accident. Failures in the defensive layers of an operational system can create gaps in defenses, some known and others unknown.

Gaps “open” and “close” as the operational situation, environment, or equipment serviceability state changes. A gap may sometimes be the result of a momentary oversight on the part of an operator, typically described as an active failure. Other gaps may represent long-standing latent failures in the system. Latent conditions exist in the system before negative effects can occur. The consequences of a latent condition may lie dormant for extended periods of time.

These gaps may occur due to:

* Undiscovered and long-standing shortcomings in the defenses,
* The temporary unavailability of some elements of the system due to maintenance action,
* Equipment failure,
* Human interaction, and/or
* Policy/decision-making.

#### 2.2.1.2 Hazard Defenses

Aviation service providers must strive to design systems that will not impose hazardous conditions during abnormal performance. Using a key systems engineering concept, such systems are referred to as being **fault tolerant**.

A fault-tolerant system includes mechanisms that will preemptively recognize a fault or error so that corrective action can be taken before a sequence of events can lead to an accident. A subset of a fault-tolerant system is a system that is designed to fail safe. A **fail-safe** system is designed such that if it fails, it fails in a way that will cause no harm to other devices or present a danger to personnel.

**Error tolerance**, another systems engineering concept, is a system attribute in which, to the maximum extent possible, systems are designed and implemented in such a way that errors do not result in an incident or accident. An error-tolerant design is the human equivalent of a fault-tolerant design.

Design attributes of an error-tolerant system include:

* Errors are made apparent,
* Errors are trapped to prevent them from affecting the system,
* Errors are detected and warnings/alerts are provided, and
* Systems are able to recover from errors.

For an accident or incident to occur in a well-designed system, gaps must develop in all of the defensive layers of the system at a critical time when defenses should have been capable of detecting the earlier error or failure. Functions, equipment, procedures interact though numerous complex relationships. Given the temporal nature of these relationships, our company must continuously monitor safety risk to maintain an acceptable level of safety performance and prevent gaps.

### 2.2.2 The Human Element’s Effect on Safety

Human error is estimated to be a causal factor in the majority of aviation accidents and is directly linked with system safety error and risk. For this reason, aviation service providers must eliminate as many errors as possible, minimize the effects of errors that cannot be eliminated, and reduce the negative effect of any remaining potential human errors.

Human performance variability is a limitation that necessitates careful and complete analysis of the potential effect of human error. Human capabilities and attributes differ in areas such as:

* Manner and ability of the senses (e.g., seeing, hearing, touching),
* Cognitive functioning,
* Reaction time,
* Physical size and shape, and
* Physical strength.

Fatigue, illness, and other factors, such as stressors in the environment, noise, and task interruption, also affect human performance. Optimally, the system is designed to resist, or to at least tolerate, human error.

When examining adverse events attributed to human error, it is often determined that elements of the human-to-system interface (such as display design, controls, training, workload, or manuals and documentation) are flawed.

The analysis of human reliability and the application of human performance knowledge must influence system design for safety systems and be an integral part of risk management. Recognizing the critical role that humans and human error play in complex systems and applications has led to the development of the human-centered design approach. This approach is central to the concept of managing human error that affects safety risk.

### 2.2.3 Closing Gaps Using SRM and SA Principles and Processes

Safety risk can be reduced proactively and reactively. Monitoring operational data, carefully analyzing the system, and reporting safety issues make it possible to proactively detect and prevent sequences of events where system deficiencies (i.e., faults and errors, either separately or in combination) could lead to an incident or accident before it actually occurs. The **same approach also can be used to reactively analyze the chain of events** that led to an accident or incident.

With adequate information, safety professionals can take corrective action to strengthen the system’s defenses when devising new policies, procedures and operations, or when making changes to them. The following example is an illustrative, but not comprehensive, list of typical defenses used in combination to close gaps in defenses:

**Equipment Defense Strategies**:

* Redundancy:
  + Full redundancy, which provides the same level of functionality when operating on the alternate system
  + Partial redundancy, which results in some reduction in functionality (e.g., local copy of essential data from a centralized network database)
* Independent checking of design and assumptions
* System design that ensures that critical functionality is maintained in a degraded mode if individual elements fail
* Policy and procedures regarding maintenance to prevent a loss of some functionality in the active system or a loss of redundancy
* Automated aids or diagnostic processes designed to detect system failures or processing errors and to report those failures appropriately
* Scheduled maintenance

**Operating Procedures**:

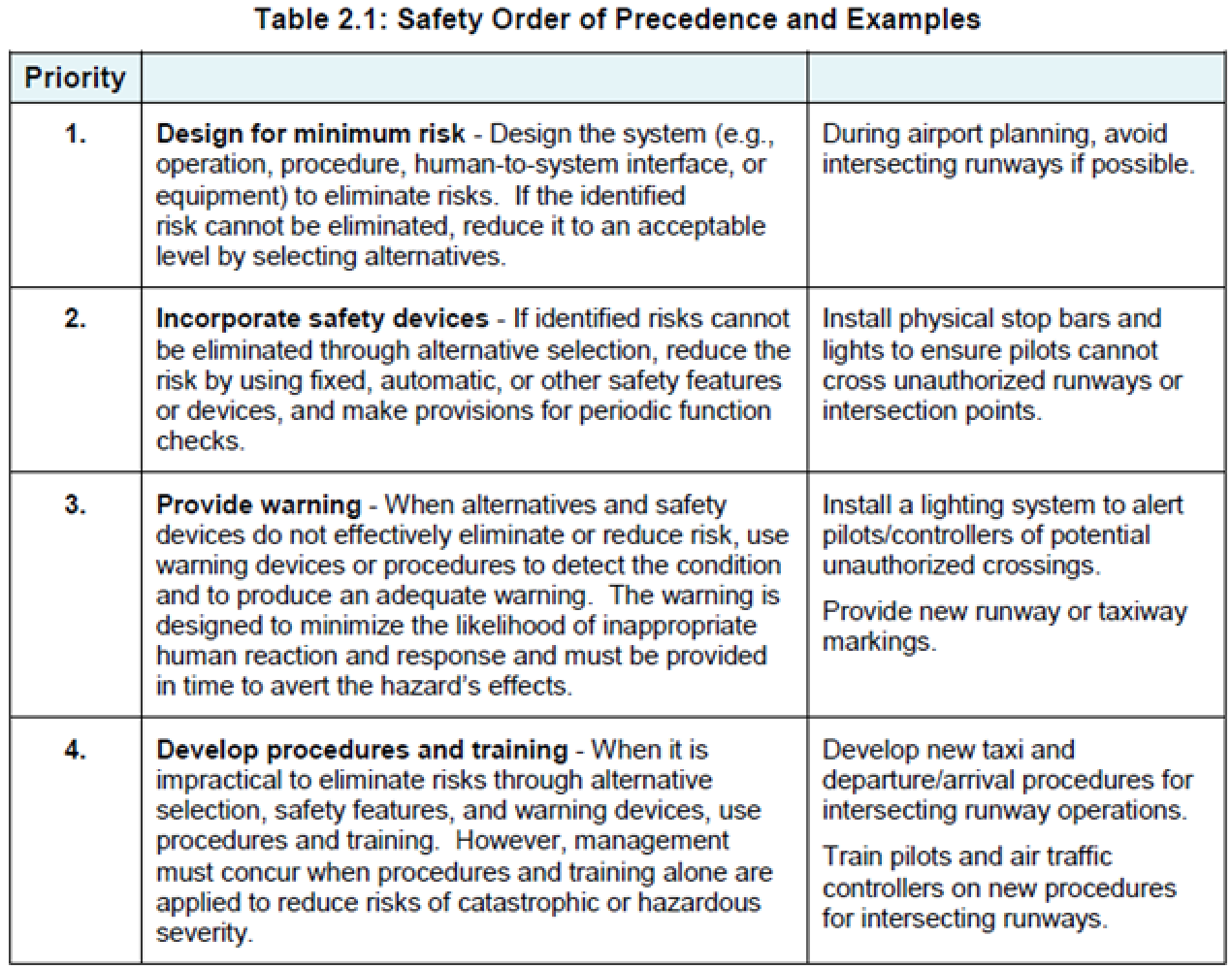
* Adherence to standard phraseology and procedures
* Read-back of critical items in clearances and instructions
* Checklists and habitual actions (e.g., requiring a controller to follow through the projected flight path of an aircraft, looking for conflicts, receiving immediate coordination from the handing-off sector)
* Inclusion of a validity indicator in designators for Standard Instrument Departures and Standard Terminal Arrival Routes
* Training, analysis, and reporting methods

**Organizational Factors**:

* Management commitment to safety
* A strong, positive safety culture
* Safety policy implementation with adequate funding provided for safety management activities
* Oversight to ensure that correct procedures are followed
* A zero-tolerance policy toward willful violations or shortcuts
* Control over the activities of contractors

### 2.2.4 Safety Order of Precedence

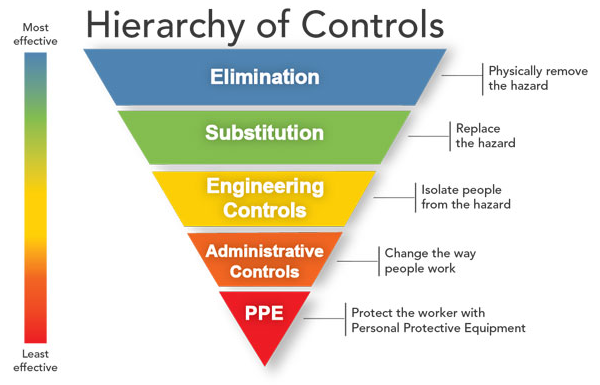
The methods for reducing safety risk generally fall under one of the four categories that make up the Safety Order of Precedence. The Safety Order of Precedence categorizes safety risk mitigations in the following order of preference:



Note: Reliance solely on training is not normally a sufficient means to mitigate safety risk.

### 2.2.5 Hierarchy of Control

Controlling exposures to operational hazards is the fundamental method of protecting employees, customers and other stakeholders. Traditionally, a hierarchy of controls has been used as a means of determining how to implement feasible and effective control solutions. A popular method for reducing safety risk fall under one of the five categories that make up the Hierarchy of Controls. The Hierarchy of Controls categorizes safety risk mitigations in the following order of preference:



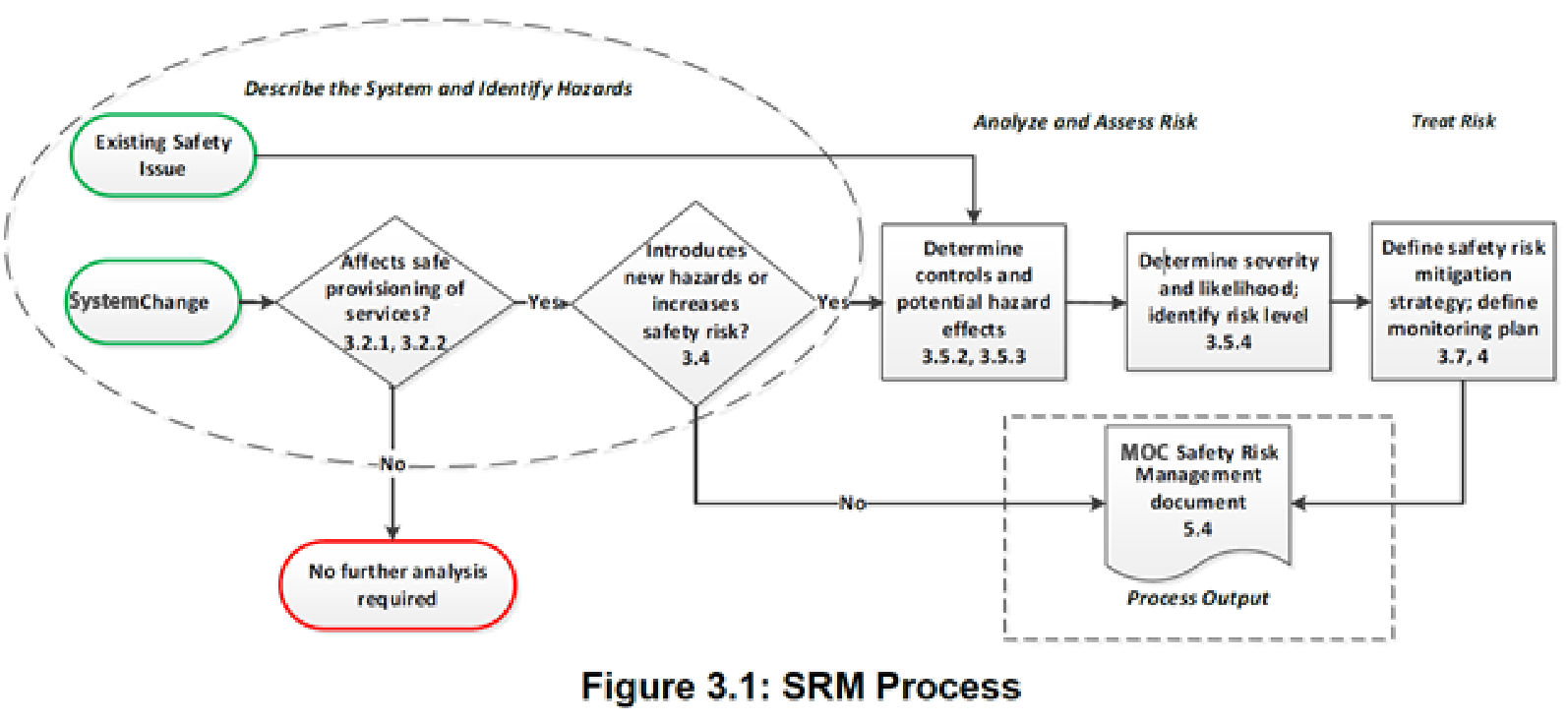
The main idea behind this hierarchy is that the control methods at the top of graphic are potentially more effective and protective than those at the bottom. Following this hierarchy normally leads to the implementation of inherently safer systems, where hazards' risk has been substantially reduced. Our SMS database uses this hierarchy to define controls in the *Proactive Hazard Analysis Tool* (PHAT).

## 3.1 Safety Risk Management (SRM) Overview

### 3.1.1 Overview of the SRM Process

This chapter provides a linear Safety Risk Management (SRM) process to follow, guidelines to identify safety hazards and mitigate their risks, and requirements for the development of consistent and thorough safety analyses. Using the steps in this chapter to perform a safety analysis will not always result in an exhaustive study of procedures, operations, or equipment (i.e., hardware and software). The appropriate level of detail in a safety analysis depends on the complexity, size, and potential effect of the change or existing safety issue.

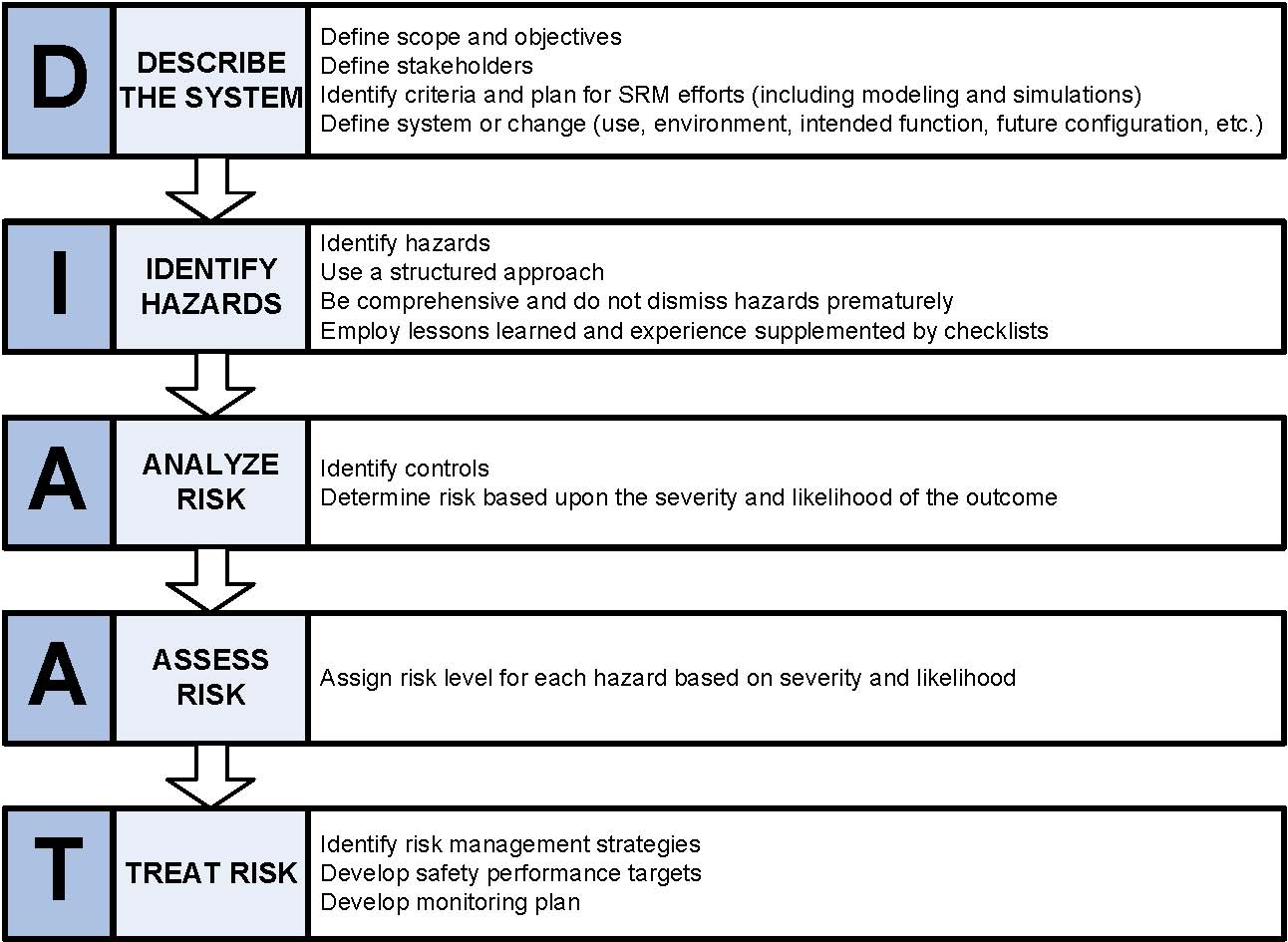
This chapter focuses solely on describing the key concepts and five phases of the safety analysis process. Refer to Section 5 and Section 6 for more detailed information on the administrative requirements regarding the development of safety documentation and the tracking of hazards and risk using the SMS database. Refer to Section 5 for SRM documentation requirements. Figure 3.1 provides a high-level depiction of the key steps, decision points, and outputs of the SRM process.



### 3.1.2 SRM Safety Analysis Phases

Performance of a safety analysis is broken down into a five-phase process, presented in Figure 3.2. Consistent with International Civil Aviation Organization (ICAO) guidelines and best practices, these five SRM phases apply to all SRM activities. Systematically completing the steps outlined in the five phases supports a thorough and consistent safety analysis.

These five phases are described in detail in Section 3.3 through Section 3.7.



**Figure 3.2 SRM Phases**

## 3.2 Scope of the SRM Process

The Safety Risk Management (SRM) process is used to assess the safety risk of changes or existing safety issues associated with company operations. These operations include the acquisition, operation, and maintenance of hardware and software; facilities management; and development of operations and procedures.

Security (e.g., physical, information, cyber), environmental, or occupational safety and health issues that potentially affect operations should be assessed during the safety analysis. These issues should not be assessed through SRM if they do not have an effect on safe operations (i.e., if they are not causes of operational safety hazards). Likewise, the SRM process is not designed to and should not be used to account for issues related to the environment, finance, budget, or labor/human resources.

Safety hazards associated with the environment, occupational safety, or security that can or do affect operations must be reported to the appropriate authority.

### 3.2.1 When to Perform a Safety Analysis

Safety analyses are most frequently performed in response to a system change. System changes may be proposed and initiated as part of implementation plans for new/modified procedures, operations, or equipment, or in response to existing safety issues currently in the system. Any employee can request a system change by submitting a “Management of Change” request in the SMS database’s *Management of Change* module.

In some cases, a safety analysis is performed in response to a request to take action on an existing safety issue or a failing risk control. Requests for action may be proposed and initiated as part of a Safety Assurance (SA) function. For our company, this is usually a result of Quality Assurance audits, or assessment findings. If a request to take action on an existing safety issue is received, a safety analysis must be performed.

Though not all system changes will require a documented safety analysis, the decision and justification to forgo performing a safety analysis is a safety decision. If there is uncertainty as to the appropriate path to take, contact the Director of Safety for assistance.

Do not use the SRM process to assess editorial or administrative changes.

The following list presents system changesthat will require a safety analysis. It is important to note that this list does not constitute a complete list or explanation of all system changes that require a safety analysis.

* Operational/procedural changes or waivers that are not defined in an existing procedure (e.g., flight trials, tests, demonstrations, and prototypes that are live in the system)
* Any waiver or change to a policy, if the policy implements a procedure that, when followed, could affect safe operations
* Introduction of new types of procedures into the system
* Addition, modification, closure, or removal of an airport, runway, or taxiway; airport building construction; and lighting changes; routes
* Our company must remain vigilant to ensure an appropriate safety assessment is conducted on construction projects to maintain continued regulatory compliance.)
* New systems used flight-related operations (or new uses for such existing systems)
* Directives that introduce new requirements and/or change requirements for risk-assessed operational systems/equipment, such as:
  + Communication, navigation, and surveillance systems
  + Weather products/services
  + Displays
  + Alerting and advisory systems
  + Service provider equipment (e.g. Broadcast, CAA Telecommunications Infrastructure)
  + Local patches
  + Decision support tools
* Changes to system certification and maintenance standards, requirements, and practices (e.g., technical handbooks)
* Deactivation, removal, or decommissioning of equipment, procedures, systems, or services
* Site adaptations, if the acceptable technical limits for such adaptations are not defined in the system-level SRM work approved prior to In-Service Decision, or if such limits are to be exceeded
* Facility changes, including:
  + Tower siting or relocation
  + Facility relocation
  + Cab replacement or redesign
  + Permanent consolidation or de-consolidation of facilities
  + Facility split
  + Temporary tower
* All charting specification changes prior to submission for final signature (e.g., symbology, color changes in routes, route identifiers)
* Route changes, including airways, sectors, and the addition or deletion of a position or sector
* Changes to policies, procedures, or system equipment for which training exists
* Establishment of or modifications to the Technical Training orders, architecture, and curricula

### 3.2.2 When a Safety Analysis May Not Be Required

#### 3.2.2.1 Overview

Not all system changes require a safety analysis using the MOC SRM process; there are exceptions. The change proponent must use the criteria in this section and Section 3.2.1 to make this determination.

A safety analysis using the SRM process does not need to be performed for system changes that are compliant with policies/processes that have undergone SRM and have been documented and approved by the appropriate management official. If these policies or procedures are changed, or if any system change deviates from these policies or procedures, a safety analysis must be performed using MOC SRM to manage the safety risk. Note that editorial and administrative changes (i.e., any changes that do not affect the substantive elements of a procedure or system) do not require SRM.

CAA and/or operational documents (e.g., policies, directives, manuals, Standard Operating Procedures, Letters of Agreement, Letters of Procedure) for developing and implementing many routine and repeatable system changes could be considered compliant with the SMS, meaning that SRM was performed, documented, and approved. For example, routine procedures such as flight inspections are conducted in accordance with [CAA Order 8200.1, *United States Standard Flight Inspection Manual*.](https://employees.faa.gov/tools_resources/orders_notices/index.cfm/go/document.information/documentID/1027073) If there are no changes to those procedures, then a safety analysis is not required. However, if there is a change to the frequency of flight inspections, a safety analysis is required.

Modifications made to systems to meet initial operational specifications may not require additional assessments if the system specifications have undergone a documented safety assessment. The modification and testing processes must also be compliant with the SMS.

#### 3.2.2.2 Management of Change Proposals

The configuration management requirements from the Management of Change Proposal process may not specifically relate to safety effects. When a system change covered by a Management of Change Proposal requires SRM, the appropriate safety analysis and documentation must be included in the material provided to the Safety Committee Review Board. In terms of SRM, a Management of Change Proposal can be categorized as one of the following:

* Not requiring any safety assessment
* Requiring a complete safety analysis by an SRM committee and an MOC SRM document (refer to Section 5)

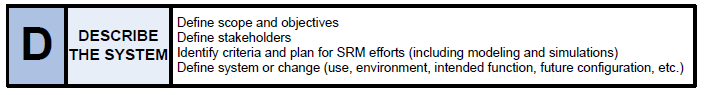
#### 3.2.2.3 Examples of Changes Unlikely to Require a Safety Analysis

The following list presents system changes that will likely not require SRM. It is not a complete list or explanation of all system changes that do not require a safety analysis.

* Changes to directives for those directives with no safety functionality
* Installation or moving of equipment if defined installation siting processes are not violated
* Maintenance actions, as specified in maintenance technical handbooks

Contact the Director of Safety for assistance determining if a safety analysis is required.

## 3.3 SRM Phase 1: Describe System



### 3.3.1 Overview

As discussed in Section 3.2.1, system changes may be proposed and initiated as part of implementation plans for new or modified procedures, operations, or system equipment, or in response to existing safety issues currently in the system.

As part of any initial decision-making and follow-on analysis, it is important to develop a detailed description of the system change and its affected elements. When deciding on the correct scope and level of detail of the safety analysis, determine the information required about the system change and/or current system.

Note: Safety analyses initiated for mitigations to existing hazards that were identified through safety audits or post-event safety risk analysis should use the issue, event or situation that led to the realization of the hazard’s effect(s) as the basis for the documented system description. Use this section as guidance; however, refer to Sections 3.4.2.1.2 and 3.4.2.1.3 for further information.

### 3.3.2 Bounding and Scoping Safety Analyses

**3.3.2.1 Bounding Safety Analyses in an Integrated System**

**Bounding** refers to limiting the analysis of a change or system to only the elements that affect or interact with each other to accomplish the central function of that change or system. In many cases, there may be a limited or incomplete understanding of the operating environment in which the system equipment, operation, or procedure will be employed, or the interconnected systems with which the changing system must be integrated for effective operation. Furthermore, the scope of assessment for other associated system equipment, operations, or procedures may be unknown. Thus, it becomes difficult to ensure that there are no gaps across the boundaries of these safety analyses. As a result, the scope may be inadvertently set at an inappropriate level.

In light of these potential difficulties, the scope of a safety analysis must be set such that gaps are eliminated. As systems become increasingly more complex, interactive, and interrelated, the assessment of potential safety risk must be integrated temporally, by domain, and across locations. It remains important to consider whether potential safety risk mitigations implemented in the short term will be adequate years into the future when other systems are introduced in the system or whether other follow-on mitigations will negate the effect of those implemented in the past.

#### 3.3.2.2 Required Depth and Breadth of the Analysis

The required depth and breadth of the safety analysis and the amount of collaboration across organizations can vary based the following factors:

* **The complexity of the system change.** The complexity and nature (i.e., operational or system acquisition) of the system change will dictate the type, depth, and number of analyses required.
* **The breadth of the system change.** The scope of an SRM activity will require additional details when the system change affects more than one division or operational area.

In general, safety analyses for more complex and far-reaching system changes will require a greater scope and more detail. When evaluating a system change, consider any potential effect on organizations outside our company (e.g., contractors, airport, landlords).

#### 3.3.2.3 Setting the Scope of the Analysis

Guidelines to help determine the scope of the SRM effort include:

* Having a sufficient understanding of system boundaries, including interfaces with peer systems, larger systems of which the system is a component, and users and maintainers;
* Determining the system elements that interact or sub-system components that may be affected; and
* Limiting the system to those elements that affect or interact with each other to accomplish the mission or function.

When setting the scope of a safety analysis:

* Define the relationships/interactions of the system change.
* Identify temporal aspects of these relationships/interactions.
* Collect safety documentation that has assessed the building blocks of the system change.
* Set the scope wide enough to determine the aggregated risk and assess any gaps.

### 3.3.3 Defining the System / System Change

#### 3.3.3.1 Describe the System and the System Change

##### 3.3.3.1.1 Overview

System descriptions need to exhibit two essential characteristics: correctness and completeness. Correctness means that the description accurately reflects the system without ambiguity or error. Completeness means that nothing has been omitted and that everything stated is essential and appropriate to the level of detail.

The system description provides information that serves as the basis for identifying all hazards and associated safety risks. The system/operation must be described and modeled in sufficient detail to allow the safety analysis to proceed to the hazard identification stage. For example, modeling might entail creating a functional flow diagram to help depict the system and its interface with the users, other systems, or sub-systems.

As discussed, the system is always a component of some larger system.

##### 3.3.3.1.2 Considerations when Defining the System

Complex system changes may require a detailed system description that includes numerous charts, drawings, design descriptions, and/or narratives. Simple system changes may only require one or two paragraphs describing the system and the system change. The description must be clear and complete before continuing the safety analysis. Questions to consider include:

* What is the purpose of the system change?
* What issue is necessitating the system change?
* How will the change be used/function in the system?
* What are the boundaries and external interfaces of the change or system?
* In what environment will the system or change operate?
* How is the system or change interconnected/interdependent with other systems?
* How will the change affect system users/maintainers?
* If the change is a waiver/renewal, how could other waivers in effect interact with it?

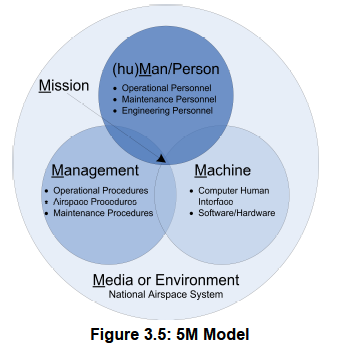
The following are examples of information to consider when describing the system:

* Fleet mix
* Number and type of operations
* Number of aircraft operated
* Operational environment (e.g., weather, political, terrain, working conditions)
* Availability and reliability of both hardware and software

Once the system elements are listed, a careful review of the change description should be conducted. A bounded system limits the analysis to the components necessary to adequately assess the safety risk associated with the change, system, and/or operation. When there is doubt about whether to include a specific element in the analysis, it is preferable to include that item, even though it might prove irrelevant during the hazard identification phase.

#### 3.3.3.2 5M Model Method

The 5M Model can be used to capture the information needed to describe the system and aid in hazard identification. The 5M Model uses a Venn diagram to depict the interrelationships among its five elements, as seen in Figure 3.5.



To adequately bound and describe a system, it is important to understand the relationships between the elements of the 5M Model.

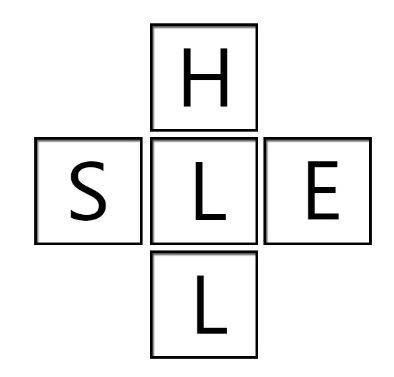
The 5M Model illustrates five integrated elements that are present in any system:

* **Mission:** The clearly defined and detailed purpose of the change proposal or system/operation being assessed
* **(hu)Man/Person:** The human operators, maintainers, and affected stakeholders
* **Machine:** The equipment used in the system, including hardware, firmware, software, human-to-system interfaces, system-to-system interfaces, and avionics
* **Management:** The procedures and policies that govern the system’s behavior
* **Media:** The environment in which the system is operated and maintained

The 5M Model and similar techniques are used to deconstruct the proposed change in order to distinguish elements that are part of or affected by the proposed change. These elements later help to identify sources, causes, hazards, and current and proposed risk mitigation strategies.

#### 3.3.3.3 SHELL Model Method

The SHELL model is a conceptual model of human factors that clarifies the scope of aviation human factors and assists in understanding the human factor relationships between aviation system resources/environment (the flying subsystem) and the human component in the aviation system (the human subsystem).



Each component of the SHELL model (software, hardware, environment, liveware) represents a building block of human factors studies within aviation.

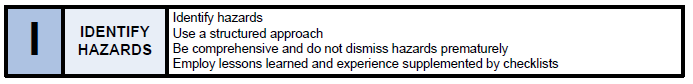
The SHELL Model can also be used to capture the information needed to describe the system and aid in hazard identification.

The human element or worker of interest is at the center or hub of the SHELL model that represents the modern air transportation system. The human element is the most critical and flexible component in the system, interacting directly with other system components, namely software, hardware, environment and liveware.

However, the edges of the central human component block are varied, to represent human limitations and variations in performance. Therefore, the other system component blocks must be carefully adapted and matched to this central component to accommodate human limitations and avoid stress and breakdowns (incidents/accidents) in the aviation system. To accomplish this matching, the characteristics or general capabilities and limitations of this central human component must be understood.

Note that each operational risk profile (ORP) in the SMS database’s **Proactive Hazard Analysis Tool** (PHAT) relies upon only one model, i.e., either 5M or SHELL. The chosen model is selected based on the preference of the Director of Safety and system’s department heads.

## 3.4 SRM Phase 2: Identify Hazards



### 3.4.1 Overview

During the hazard identification phase, identify and document safety issues, their possible causes, and corresponding effects. A **hazard** is defined as any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a prerequisite to an accident or incident.

Our company is responsible for identifying and mitigating hazards with unacceptable risk (i.e., high risk). Likewise, our company should determine if hazards with acceptable risk (i.e., medium and low risk) can be further mitigated. The hazard identification stage is integral to all preliminary safety analyses and follow-on, in-depth analyses in determining the appropriate means to address any safety risks associated with a system change. At this point, decide whether the Management of Change (MOC) Safety Risk Management (SRM) document will contain a safety analysis finding with or without hazards (refer to [Section 5.4)](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS5_4.pdf). Refer to [Section 3.7.2](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS3_7.pdf) for further discussion of risk reduction strategies. Refer to [Section 6](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS6_1.pdf) for guidance on the signatures required for implementation of the system change.

The following resources and methods can be used to identify hazards:

* Safety analysis accompanying the proposed implementation of a new or modified operation, process, or piece of system equipment;
* Operations Safety Program reports;
* Trending Chart reports;
* Key performance indicator frequency reports;
* Regulatory compliance audits;
* Risk Analysis Processes;
* Regulatory or client safety recommendations;
* Audits performed as part of facility-level Quality Control efforts or Safety and Quality Assurance efforts; and
* Reports of unsafe conditions in daily operations.

Refer to [Section 7](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS7_1.pdf) for information about the various audit and reporting programs and tools.

### 3.4.2 Potential Sources of Hazards

The hazard identification stage considers all possible causes of hazards. The use of previous hazard analyses when identifying hazards is important, as it can reduce the time needed to identify hazards and also provides consistency in SRM. For example, approved MOC SRM documents on similar changes or earlier integrated assessments, including applicable cross-organizational safety assessments, may be useful. In PHAT, a section exists to review “Related Management of Change Projects.” These MOC projects are useful to identify previously reviewed hazards and related hazard documentation.

Depending on the nature and size of the system under consideration, the causes of hazards may include:

* System equipment failure/malfunction,
* Operating environment (including physical conditions, airspace, and route design),
* Human operator failure/error,
* Human-machine interface problems,
* Operational procedures limitations/design,
* Maintenance procedures limitations/design, and/or
* External services.

#### 3.4.2.1 Existing Hazards

An existing hazard is any hazard that is currently in the system, such as the *Hazard Register,* *Goals and Objectives* KPI Objectives’ History, or listed in the Top 5 *Executive Dashboard* charts. Existing hazards often fall into the following categories:

##### 3.4.2.1.1 Identified but Not in the Scope of an Ongoing System Change

These hazards must typically be addressed through a separate, follow-on safety analysis performed by the organization or department deemed responsible. The Director of Safety can assist in determining the organization or department responsible for assessing existing identified hazards. By default, department heads with risk acceptance authority over their area of operations is responsible for ensuring hazards are properly documented and risk is accepted.

##### 3.4.2.1.2 Hazards Identified by Audits

When an audit identifies a potential safety issue, the issue must be addressed using a corrective action plan that identifies means to reduce safety risk. If there are potential changes to the system, those changes must go through the MOC SRM process.

##### 3.4.2.1.3 Hazards Identified by Top 5

When the Top 5 Program identifies safety issues, the safety issues must be addressed using a corrective action plan that identifies means to reduce safety risk. If there are potential changes to the system, those changes must go through the MOC SRM process. As with safety risks identified in MOC SRM documents, risk treated through a corrective action plan must be monitored. This requires determining the appropriate risk level using the matrix in this manual (see [section 3.6)](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS3_6.pdf#page=2&zoom=66.6656,68,796), documenting the predicted residual risk (such as in PHAT), creating safety performance targets (or other means to measure safety performance) and monitoring activities, and obtaining approval for risk acceptance and implementation. Refer to [Section 4.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS4_3.pdf#page=1&zoom=auto,70,720) for more information on monitoring and [Section 6](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_1.pdf#page=1&zoom=auto,70,720) for more information on risk acceptance and approval.

##### 3.4.2.1.4 Emergency Modifications

There may be unusual, unforeseen, or extraordinary issues or conditions that require the implementation of hardware or software solutions in a timeframe that does not allow proceeding through the formal MOC SRM process. Emergency modifications are temporary fixes installed to maintain operational continuity during unusual or emergency conditions. Such system changes may result from unforeseen natural occurrences, a lack of replacement parts, software patches, or real-time situations that require immediate action. Refer to [Section 5.5.2](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS5_5.pdf#page=1&zoom=auto,70,390) for information on how to properly document emergency modifications.

##### 3.4.2.1.5 Existing High-Risk Hazards

When our company’s Director of Safety validates an existing hazard as high risk, he or she must notify our company’s Accountable Executive and safety committee of the high risk and the interim actions needed to mitigate the risk. Our company’s Director of Safety must approve the interim action and accept the associated risk or require the operation to be stopped. The responsible operational department must coordinate with our company’s Director of Safety to address the risk and any potential corrective actions. Refer to [Section 3.7.2](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS3_7.pdf) for risk management strategies. Refer to [Section 5.5.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS5_5.pdf#page=1&zoom=auto,70,161) for information on the administrative process of addressing existing high-risk hazards and obtaining approval for their risk reduction.

### 3.4.3 Elements of Hazard Identification

When considering new equipment and procedures or planned modifications to current equipment and procedures, define the data sources and measures necessary to identify hazards. The elements of a thorough system description contain the potential sources of hazards associated with the proposed change. There are numerous ways to do this, but all require at least three elements:

* Operational expertise that relates specifically to the operation or equipment,
* Training or experience in various hazard analysis techniques, and
* A defined hazard analysis tool, such as the Proactive Hazard Analysis Tool (PHAT).

#### 3.4.3.1 Techniques for Hazard Identification and Analysis

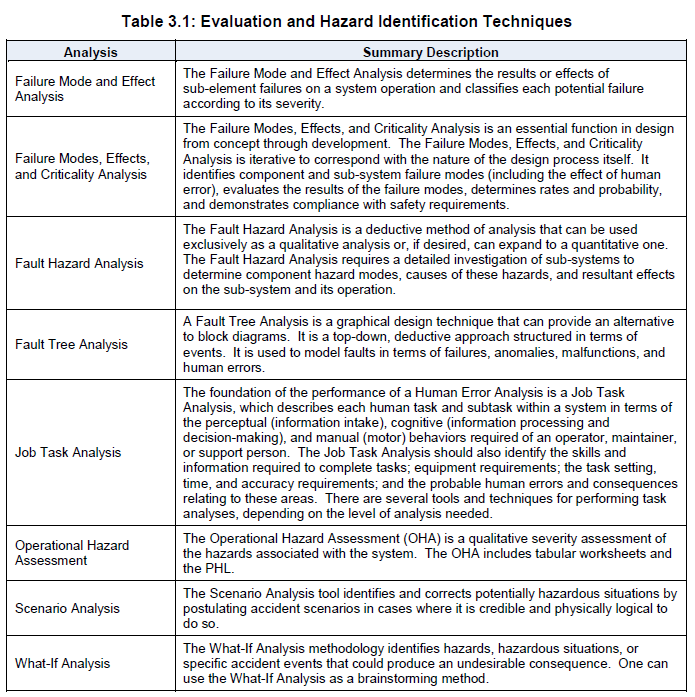
In many cases, to identify and analyze safety hazards, a Preliminary Hazard List (PHL) in the *Proactive Hazard Analysis Tool* (PHAT) will suffice. Some cases, however, may require other tools or techniques (refer to Section 3.4.3.1.2).

##### 3.4.3.1.1 Developing a PHL

The process of describing the system using a tool like the 5M Model or the SHELL Model is designed to facilitate brainstorming for sources of hazards. The next step in the hazard identification process is to develop a PHL. The **PHL** may be a combination of hazards, causes, effects, and system states for the operational risk profile (ORP). The resulting hazards, causes, effects, and system states will then be placed automatically into the *Hazard Risk Register* via the PHAT.

##### 3.4.3.1.2 Other Accepted Tools and Techniques

If the safety analysis calls for an additional means to identify hazards and compare solutions, select the methodology that is most appropriate for the type of system being evaluated. The Director of Safety can provide additional guidance on which tool(s) to use for various types of system changes (refer to Table 3.1).



When selecting hazard identification/analysis tools, it is important to consider:

* The necessary information and its availability;
* The timeliness of the necessary information;
* The amount of time required to conduct the analysis; and
* The tool that will provide the appropriate systematic approach for:
  + Identifying the greatest number of relevant hazards,
  + Identifying the causes of the hazards,
  + Predicting the effects associated with the hazards, and
  + Assisting in identifying and recommending risk management strategies.

### 3.4.4 Causes and System State Defined

Identify and document potential safety issues, their possible causes, and the conditions under which the safety issues are revealed (i.e., the system state).

**Causes** are events occurring independently or in combination that result in a hazard or failure. They include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

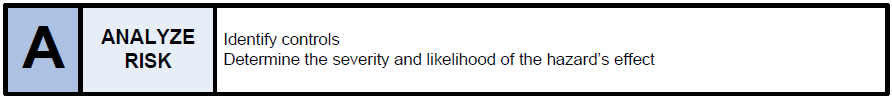
A **system state** is the expression of the various conditions (characterized by quantities or qualities) in which a system can exist. It is important to capture the system state that most exposes a hazard, while remaining within the confines of any operational conditions and assumptions defined in existing documentation. The system state can be described using a combination of, but not limited to, the following terms:

* **Operational and Procedural:** Simultaneous procedures versus visual approach procedures, etc.
* **Conditional:** Peak traffic versus low traffic, etc.
* **Physical:** Electromagnetic environment effects, precipitation, primary power source versus back-up power source, closed runways versus open runways, dry runways versus contaminated runways, environmental conditions, etc.

Any given hazard may have a different risk level in each possible system state. Hazard assessments must consider all possibilities while allowing for all system states. In a hazard analysis, it is important to capture different system states when end results lead to the application of different risk reduction methods and tools. In the SMS database PHAT, use the section labelled “Rationale for listing & assessing risks” to briefly describe considered “system states.”

System states may be further detailed during the system description using either the 5M or SHELL models. PHAT accommodates both models to assist in adequately describing the system.

## 3.5 SRM Phase 3: Analyze Risk



### 3.5.1 Overview

An accident or incident rarely results from a single failure or event. Consequently, risk analysis is seldom a binary (e.g., on/off, open/closed, broken/operational) process. Risk and hazard analyses can identify failures from primary, secondary, or even tertiary events.

During the risk analysis phase:

* Evaluate each hazard (identified during the “Identify Hazards” phase) and the system state (from the “Describe the System” and “Identify Hazards” phases) to determine the controls,
* Analyze how the operation would function should the hazard occur, and
* Determine the hazard’s associated severity and likelihood and provide supporting rationale.

### 3.5.2 Controls

A **control** is anything that currently reduces a hazard’s causes or effects. Policies, procedures, hardware, software, or other tools can only be considered controls if they are part of the system and have demonstrated effectiveness. Understanding controls affects the ability to determine credible effects. Do not document safety requirements as controls; safety requirements are only planned or proposed ways to reduce risk. Refer to [Section 3.7.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS3_7.pdf#page=3&zoom=auto,70,670) for information about documenting safety requirements. Controls should have the appropriate status and hierarchy of control assigned in PHAT. Valid statuses include:

* Implemented – currently in use;
* Scheduled – planned and not affecting operations; and
* Awaiting completion- currently affecting operations, but not fully implemented.

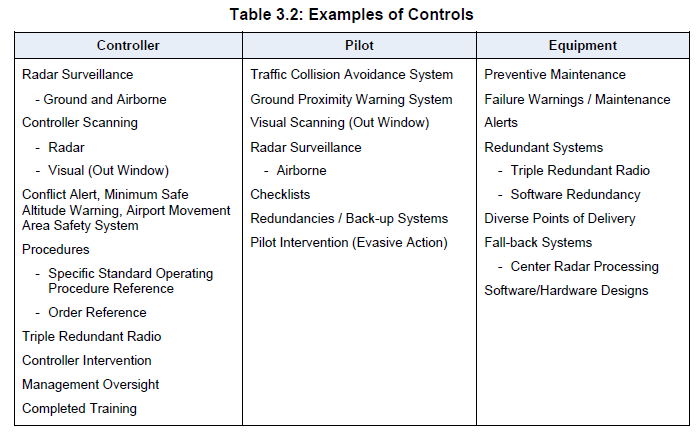
Hierarchy of Control is a technique used to prioritize controls according to their effectiveness. Use the Hierarchy of Control to communicate effectiveness to managers. Consider elimination of hazard before any other options for implementing controls.

* **Elimination** – Physically remove the hazard
* **Substitution** – Replace the hazard
* **Engineering** controls – Isolate people from the hazard
* **Administrative** controls – Change the way people work
* **Personal protective equipment**– Protect the worker with PPE

Provide supporting data and/or a rationale that confirms the control’s use, applicability, and availability related to the hazard in PHAT. Document these elements in the available “Description” and “Comments” fields in PHAT. For instance, if documented procedures are identified as controls, cite the specific version, paragraph, and/or section number(s). Alternatively, if equipment is identified as a control, discuss how it reduces or manages the risk. When considering a change, only document the controls associated with the change under evaluation in the MOC SRM document. List controls in the “Mitigation” section of the MOC SRM document’s “Hazard Identification Analysis.”

When considering existing hazards identified through safety audits or post-event risk analysis, consider any control(s) that either minimized the hazard’s effect or failed. These controls are listed in the *Proactive Hazard Analysis Tool* (PHAT) under the respective hazard. When undocumented controls are discovered, contact the process owner listed for the respective Hazard Category in PHAT.

Table 3.2 provides broad examples of controls. This is not a comprehensive list of controls; each identified control should be directly applicable to the hazard being addressed.



### 3.5.3 Determining a Credible Hazard Consequence or Effect

**Effect** refers to the real or credible harmful consequence that has occurred or can be expected if the hazard occurs in the defined system state. A single hazard can have multiple effects. **Credible** means that it is reasonable to expect that the assumed combination of conditions that define the system state will occur within the operational lifetime of a typical system. Credible effects should be determined with respect to controls. Document all identified credible effects in PHAT under the “Hazard-related Consequences” section for the respective hazard.

Often, there is confusion when distinguishing the *possible* effects of a hazard from the *credible* effects; possible is not necessarily the same as credible. The credibility of an effect is a nuanced and key consideration in the analysis. A thorough understanding of this concept can save time in determining the risk level of a specific hazard. When determining the credibility of the effect, it is important to:

* **Recall and Understand the Defenses in Depth Model.** It is well established that incidents and accidents cannot typically be attributed to a single cause, or even to a single individual. Rather, aviation safety issues are the end result of a number of causes. Based on this model (see [Section 2.2.1)](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS2_2.pdf#page=1&zoom=auto,70,594), it is critical to consider the defenses that already exist in the system when deciding the credibility of an effect.
* **Review History.** Check the historical record. Have there been similar issues reported in the system or similarly implemented changes? What happened? How does the experience gained from the activities affect the credibility of the outcomes that have been identified for a proposed change?
* **Rely on Quantitative Data.** Section 3.5.4.3.3 and Section 3.5.4.3.4 discuss the use of quantitative and qualitative data, respectively. Do the quantitative data support the credibility of the outcomes identified? If so, the hazard severity determination can be based on statistical data, and the safety assessment will be more objective.
* **Visualize the Occurrence of the Accident or Incident**. Put the hazard in its proper context within the given system state and determine the sequence of events (causes) that could lead to the **worst credible outcome**. Given that aviation service providers strive to build error-tolerant systems (in accordance with the Defenses in Depth Model), consider how many controls (redundancies, procedures, warning devices, equipment, etc.) would have to fail in series so that an identified hazard breaches every defense to result in a catastrophic event. Is it reasonable (i.e., credible) to expect that the necessary combination of extreme conditions will simultaneously occur within the operational lifetime of the system?

### 3.5.4 Defining Risk

#### 3.5.4.1 How to Define and Determine Risk

**Risk** is the composite of predicted severity and likelihood of the potential effect of a hazard. While the worst credible effect may produce the highest risk, the likelihood of the worst credible effect is often very low. A less severe effect may occur more frequently and therefore present a higher risk than the more severe effect. The ways to reduce the risk for the two effects may be different, and both must be identified. Consider all credible effects and their associated risks in order to identify the highest risk for the safety hazard.

Attempt to obtain and document objective evidence (e.g., historical evidence of similar changes, testing data, modeling or simulation results) to support the assessed level of risk. If quantitative data are not available, document the research methods—including the data sources reviewed—in addition to qualitative assessments. Because different system states can affect both severity and likelihood in unique ways, determine whether the hazard will exist in several system states and assess the risk accordingly.

#### 3.5.4.2 Determining Severity

**Severity** is the consequence or impact of a hazard’s effect or outcome in terms of degree of

loss or harm. It is independent of likelihood and must be determined before likelihood is calculated. Assess all effects and consider controls when determining severity, and use the measure yielding the most conservative estimate (i.e., the higher severity). Table 3.3 is the severity table used by our company to assess the severity of a hazard when performing Safety Risk Management (SRM) and Safety Assurance (SA) activities. Provide a rationale for the chosen severity level in the *Proactive Hazard Analysis Tool* (PHAT) in the respective hazard under the section labelled “Rationale for listing and assessing risks.”. For reported issues and audit findings in the SMS database, document rationale in the “Assessment Justification” section on the Assess tab in *Issue Manager*.

**Table 3.3: Hazard Severity Definitions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Hazard Severity Classifications** | | | | |
|  | **Catastrophic**  **A** | **Critical**  **B** | **Significant**  **C** | **Marginal**  **D** | **Negligible**  **E** |
| **Personnel** | Multiple Fatality | Single Fatality | Serious Injury | Minor Injury | Slight/No Injury |
| **Environment** | Massive Effect | Major Effect | Localized Effect | Minor Effect | Slight/No Effect |
| **Material** | Extensive Damage | Major Damage | Local Damage | Minor Damage | Slight/No Damage |
| **Mission** | Total Mission Failure | Multiple significant mission element failures | Single significant mission element failure | Certain mission element failures | Minor Degradation |

##### 3.5.4.2.1 Assessing Severity of Equipment Hazard Effects

When performing a safety analysis on company equipment that was previously assessed, it is recommended to use the data, methodology, and results of the previous work as the starting point for the new safety analysis. If there are differences in functionality between the original, previously assessed system and the system undergoing analysis, the differences should be accounted for and documented in the new safety analysis.

In general, equipment can fail such that one of two effects are expected:

* **Loss of Function.** The service is no longer provided.
* **Malfunction.** The service is being provided inaccurately or with diminished integrity.

When identifying functional failures that lead to hazards, the loss of function and the malfunction of constituent parts must be considered. The severity of malfunctions and losses of function from infrastructure systems, such as telecommunications and power systems, is dependent upon the services they support.

Examples of the systems that provide services include, but are not limited to, the following:

**Navigation (NAV)**

* *Instrument approach systems*: Localizer, glide slope (e.g., Visual Glide Slope Indicators, such as Precision Approach Path Indicator and Visual Approach Slope Indicator), markers, approach lights, Distance Measuring Equipment, Localizer-type Directional Aid, and Runway Visual Range
* *En route guidance systems*: Very-high Frequency Omnidirectional-range Radio, Distance Measuring Equipment, and Wide-area Augmentation System

**Communication (COMM)**

* *Air-to-ground COMM*: Headsets/microphones, speakers, voice switches, radio control equipment, and radios
* *Ground-to-ground COMM*: Headsets/microphones, speakers, and voice switches

**Surveillance**

* Automatic Dependent Surveillance, Airport Movement Area Safety System, Airport Surface Detection Equipment, and radar automation and display

**Weather**

* Automated Surface Observing System, Automated Weather Observing System, Low-Level Wind Shear Alert System, Flight Service automation system, Operations and Supportability Implementation System

#### 3.5.4.3 Determining Likelihood (Probability)

##### 3.5.4.3.1 Likelihood versus Frequency

**Likelihood** is defined as the estimated probability or frequency, in quantitative or qualitative terms, of a hazard’s effect or outcome. More specifically, the concept of likelihood can be separated into two components: likelihood/probability and frequency. Likelihood is a rate of how often a given effect is expected to occur. **Frequency** is how often a given effect occurs. Frequency is a known value, while likelihood is a prediction. Use frequency (known value) to assess the current or residual risk (see [Section 4.3.1](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS4_3.pdf#page=1&zoom=auto,70,570) and [Section 4.3.4) and likelihood](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS4_3.pdf#page=1&zoom=auto,70,153) (predicted value) when assessing initial and predicted residual risk. Provide a rationale for the likelihood chosen in the PHAT or when assessing risk for reported issues and audit findings.

##### 3.5.4.3.2 What to Consider When Defining Likelihood

**Frequency and Modeling**

Frequency is sometimes used to help estimate likelihood, but historical data do not always represent future conditions. Historical frequency may be zero for a given procedure, but that does not mean that the future likelihood is also zero. For example, a facility may conduct a procedure that has unreported incidents that could lead to an undesirable outcome, such as a loss of separation or a collision. Likewise, a facility may not have encountered the scenario or system state that exposes the more severe outcome. Consider all potential effects that are derived from indicators of the operation in all credible risk scenarios. This practice is required to

challenge the philosophy of, “It has not happened in the past, so it will not happen in the future.”

When possible, use modeling to examine the effects of hazards that are too rare to have significant historical statistical data available. If modeling is required and data are available, the risk assessment should be based on statistical or observational data (e.g., radar tracks). Where there are insufficient data to construct statistical risk assessments, input from Subject Matter Experts (SMEs) can be used. This means that if the true rate of a particular type of operation is unknown, it can be estimated using expert judgment. It is important to note that complex proposed system changes require quantitative data to support the associated risk analysis.

**Credible Effects and Controls**

Analyze the likelihood of all credible effects to:

* Determine the highest potential risk; and
* Identify all system states that expose the risk.

Remember that less severe effects may occur more frequently, producing a higher risk, which is why it is important to determine the likelihood of all credible effects.

Always consider controls when determining likelihood because they may minimize the likelihood of an effect.

##### 3.5.4.3.3 Calculating Likelihood with Quantitative Data

Once the credible effects and the estimated rates of occurrence have been determined, it is possible to calculate a likelihood rating. The SMS Pro database is the primary source to analyze operational safety data.

To estimate the likelihood, first determine the expected number of times the credible effect will occur (i.e., the number of times that the hazard will occur in the system state that will expose the risk). Finally, compare the result of this calculation (presented below) to the ranges presented in Table 3.5 to determine the likelihood rating.

**Table 3.5 Likelihood of Effect**

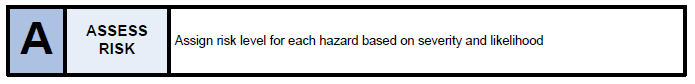
|  |  |
| --- | --- |
| **Frequent** | Reported > 3x/year at Location |
| **Probable** | Reported > 3x/year in Company |
| **Remote** | Happened before in Company |
| **Extremely Remote** | Known in the Industry |
| **Extremely Improbable** | Unknown in the Industry |

##### 3.5.4.3.4 Determining Likelihood When No Data Are Available

For some changes or for reported issues and audit findings, the necessary data for evaluating likelihood are not available. There may not be a similar enough change/procedure/situation in the system to provide similar data from which to estimate a rate of occurrence. In situations where modeling is not feasible, pure subject matter expertise is the only input available, providing a qualitative approach to determining likelihood.

Relying solely upon subject matter expertise is only recommended when all avenues of data collection have been exhausted or when the change proponent is attempting to implement a new operation for which no data exist. For a majority reported issues and proposed changes in the system, SMEs can collect and analyze data from similar companies to determine the number of expected occurrences of an effect.

## 3.6 SRM Phase 4: Assess Risk



### 3.6.1 Overview

In this phase, identify each hazard’s associated initial risk and plot each hazard on a risk matrix.

When assessing and mitigating safety risk, first determine the risk level prior to the implementation of any safety requirements (see Section 3.7.3). **Initial risk** describes the composite of the severity and likelihood of a hazard, considering only *fully implemented* controls and documented assumptions for a given system state. It describes the risk before any of the safety requirements are implemented.

When assessing equipment or existing hazards, the initial risk may be equated to the **current risk**, which is defined as the assessed severity and frequency of a hazard’s effects in the present state.

### 3.6.2 Risk Levels and Definitions

Record all hazards and their associated risk levels in the Proactive Hazard Analysis Tool (PHAT). Risk assessments for reported issues and audit findings in the SMS database are managed on the “Assess” tab in *Issue Manager*. Hazards’ risks are assigned one of three risk levels:

**3.6.2.1 Unacceptable – High Risk**

This is unacceptable (high) risk. Proposed change either cannot be implemented or operations cannot continue unless the hazard’s associated risk is mitigated to “Mitigatable” (medium) or “Acceptable” (low). Existing high-risk hazards also must be reduced to medium-or low-risk hazards. The predicted residual risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact to the hazard’s causes or effects. When documenting “predicted residual risk,” use the associated section in PHAT for each hazard monitored.

Hazards with catastrophic effects that are caused by single point events or failures, common cause events or failures, or undetectable latent events in combination with single point or common cause events are considered high risk, even if the possibility of occurrence is extremely improbable.

When a system has a **single point failure**, there is a failure of one independent element of the system that causes or could cause the whole system to fail. The system does not have a back-up, redundancy, or alternative procedure to compensate for the failed component. An example of a single point failure is found in a system with redundant hardware, in which both pieces of hardware rely on the same battery for power. In this case, if the battery fails, the entire system will fail.

A common cause failure is a single fault resulting in the corresponding failure of multiple components. An example of a common cause failure is found in a system with redundant computers running on the same software, which is susceptible to the same software bugs.

#### 3.6.2.2 Mitigatable – Medium Risk

Although initial mitigatable (medium) risk is acceptable, it is recommended and desirable that safety requirements be developed to reduce severity and/or likelihood. Associated risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact to the hazard’s causes or effects. Refer to Section 4.2 for information on monitoring.

A catastrophic severity and corresponding extremely improbable likelihood qualify as mitigatable risk, provided that the effect is not the result of a single point or common cause failure. If the cause is a single point or common cause failure, the hazard is categorized as unacceptable risk.

#### 3.6.2.3 Acceptable – Low Risk

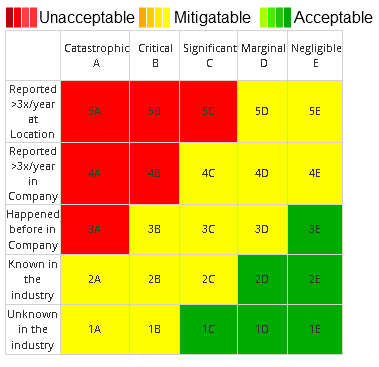
This is acceptable risk without restriction or limitation. It is not mandatory to develop safety requirements for low-risk hazards; however, best practices will have us develop a monitoring plan with at least one safety performance target when time permits.

Reported issues with associated “acceptable” risk assessments require no future review dates to be set. Furthermore, these reported issues require no firm “targeted closure date” to be set in the database. In order to keep the database tidy, all issues are required to be closed; however, no firm deadline is required for reported issues with acceptable risk assessments.

### 3.6.3 Plotting Risk for Each Hazard, Reported Issue or Audit Finding

The risk matrix shown in Figure 3.7 is used to determine risk levels. Plotting the risk for each hazard, reported issue or audit finding on the matrix helps to prioritize treatment. The rows in the matrix reflect the likelihood categories, and the columns reflect the severity categories.

**Figure 3.7: Risk Matrix**



Adhere to the following guidelines when plotting risk for each hazard:

* Plot a hazard’s risk according to its associated severity and likelihood.
* To plot the risk for a hazard on the risk matrix, select the appropriate severity column (based on the severity definitions in Table 3.3) and move down to the appropriate likelihood row (based on the likelihood definitions used from Table 3.5).
* Plot the hazard in the box where the severity and likelihood of the effect associated with the hazard intersect.
* If the plotted box is red, the risk associated with the hazard is “Unacceptable” (high); if the box is yellow, the risk associated with the hazard is “Mitigatable” (medium); and if the box is green, the risk associated with the hazard is “Acceptable” (low.)

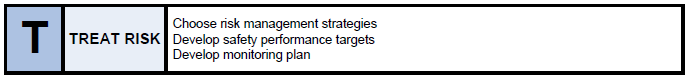
### 3.6.4 Risk Acceptance Decision-Making Authority - Reactive

For issues not relating to Management of Change (MOC) Safety Risk Management (SRM) activities, the following table (3.6) illustrates management authority to accept risk or the performance of risk controls based on the scope of the risk and on identified risk level. MOC SRM risk acceptance authority can be found in Table 6.1 Signatures for MOC Approval and Risk Acceptance.

**Table 3.6 Risk Acceptance for Reactive Issues and Risk Controls**

|  |  |  |
| --- | --- | --- |
| **Safety Risk and/or Controls** | **Unacceptable Risk** | **Mitigatable or Acceptable Risk** |
| Limited to Local Service Unit or Division | Department Head of Local Service Unit | Any mid-level or above manager in service unit |
| Spans Multiple Service Units or Divisions | All Dept Heads of Affected Service Units | At Least Two Dept Heads of Affected Service Units |
| System-wide | Accountable Executive | At Least Two Dept Heads of Affected Service Units |
| Affects outside stakeholders | Accountable Executive | Any Dept Head of Affected Service Units |

## 3.7 SRM Phase 5: Treat Risk



### 3.7.1 Overview

In this phase, identify appropriate means to mitigate or manage the safety risk. Treating risk involves:

* Identifying appropriate safety requirements (safety plan),
* Defining safety performance targets or a sound alternate method to verify the predicted residual risk for each hazard, and
* Developing a monitoring plan that prescribes tasks and review cycles for comparing the current risk to the predicted residual risk.

### 3.7.2 Risk Management Strategies

To address safety risk, identify and evaluate means that either manage the risk or reduce it to an acceptable level. The four risk management strategies are

1. risk control,
2. risk avoidance,
3. risk transfer, and
4. risk assumption.

Assess how the proposed risk management strategy affects overall risk. Consider using a combination of actions to best manage or reduce the risk to an acceptable level. When determining the appropriate strategy, consider how the safety performance target (see Section 4.1) will be used to evaluate the safety performance of the chosen course of action.

#### 3.7.2.1 Risk Control

A **risk control strategy** involves the development of **safety requirements**, defined as planned or proposed means to reduce a hazard’s causes or effects. Examples include policies or procedures, redundant systems and/or components, and alternate sources of production. Refer to Section 3.7.3 for information on developing safety requirements.

An explanation of how a safety requirement reduced the hazard’s risk level—ultimately supported with objective evidence through testing, monitoring, or another method—must be provided for each safety requirement. When using the SMS database to document management of change activities, safety requirements should be documented in the “Mitigation” section of the respective MOC SRM document. All safety requirements that are implemented and are determined to have successfully addressed the hazard or safety issue become part of the system. At that time, they will be considered “controls” that form the basis for future safety hazard and risk analysis efforts. Implemented controls for each relevant hazard must be documented in *PHAT* to facilitate monitoring during Safety Assurance (SA) activities. Refer to Section 3.5.2 for information on controls.

##### 3.7.2.1.1 Evaluate Effectiveness of Safety Risk Controls

Twice each year, Director of Safety shall evaluate the effectiveness of identified safety risk controls in *PHAT*. Controls will be evaluated using the SMS database’s Hazard Risk Register, which has the ability to identify both effective and ineffective controls when used properly. When ineffective controls are discovered, the Director of Safety will ensure these controls are flagged for review by the Department Head in charge of the affected operational area. The list of controls flagged for review are listed in the SMS database’s *Custom Report Viewer* under the “**Control Measures Flagged for Audit**.”

Controls are continuously monitored during the reactive and proactive risk management processes. When reported issues are classified using hazards from the Hazard Register, management can immediately evaluate control measures related to the associated hazard.

The safety team and responsible manager will review control measures’ effectiveness during the classification process of each issue processed in the SMS database *Issue Manager*. Evaluating hazard’s effectiveness during the treatment of reported issues is performed on the Classify or Manage tab in *Issue Manager*.

#### 3.7.2.2 Risk Avoidance

The **risk avoidance strategy** averts the potential occurrence and/or consequence of a hazard by either selecting a different approach or not implementing a specific proposal. This technique may be pursued when multiple alternatives or options are available, such as determining where to route aircraft during emergencies.

In some cases, a decision may be made to limit changes to certain conditions or system states, thereby avoiding the risk associated with other conditions. An example of this is allowing simultaneous operations on one runway that is over-flown by three other runway flight paths. It may be discovered that the risk associated with the simultaneous operation can be mitigated to an acceptable level for two of the runways but not for the third. It may be decided that aircraft will not be allowed to operate on the third runway while simultaneously landing on the crossing runway, thereby avoiding risk.

A Comparative Safety Assessment may be used when multiple systems or procedures are available. If one alternative cannot be mitigated to an acceptable level, then another system, method, or procedure may be chosen. When no alternatives are available, the risk avoidance strategy is more likely to be used as the basis for a “go” or “no-go” decision at the start of an operation or program. Risk must be avoided from the perspective of all affected stakeholders. Thus, an avoidance strategy is one that involves all of the stakeholders associated with a proposed change or when treating reported issues or audit findings.

#### 3.7.2.3 Risk Transfer

The **risk transfer strategy** shifts the ownership of risk to another party; the recipient may be better equipped to mitigate the risk at the operational or organizational level. Organizations transfer risk primarily to assign responsibility to the organization or operation most capable of managing it. The recipient must accept the risk, and the transfer must then be documented (e.g., through a Letter of Agreement, Statement of Agreement, or Memorandum of Agreement).

Examples of risk transfer may include:

* The development of new policies or procedures to change ownership of a system component to a more appropriate organization,
* The procurement of contracts for specialized tasks from more appropriate sources (e.g., contract maintenance), and
* The transfer of maintenance operations from the parent organization to another organization that provides maintenance.

Transfer of risk cannot be the only method used to treat a high-risk hazard. Identify safety requirements to lower the safety risk to medium or low before it can be accepted in the system. All transferred risks must be monitored until the predicted residual risk is verified by the appropriate organization.

#### 3.7.2.4 Risk Assumption

The **risk assumption strategy** simply means accepting the risk. The risk acceptor assumes responsibility for the risk as it is. When a risk acceptor agrees to implement a system change, he or she agrees to implement it based on the predicted residual risk being medium or low and assumes responsibility for the risk. When this management strategy is used, the predicted residual risk is derived from the controls. Under this strategy, controls serve as the basis on which safety performance targets or alternate methods to verify predicted residual risk are developed. *It is recommended and desirable that safety requirements be developed to further mitigate risk or reduce likelihood or severity.*

It is not permissible to use a risk assumption strategy to treat an initial or current high risk associated with a hazard. The predicted residual risk for initial high-risk hazards must be medium or low before it can be accepted into the system.

### 3.7.3 Documenting Safety Requirements

All safety requirements identified by the Safety Risk Management (SRM) committee and included in the Proactive Hazard Analysis Tool (PHAT) are considered to be recommendations for review and approval by the appropriate signatories. After appropriate means of managing risk have been developed and documented by the SRM committee, management officials may identify the effect of safety requirements on other organizations and coordinate with the affected organizations.

It may be necessary to perform separate safety analyses on the safety requirements to determine their effects on the system. If so, the associated safety analyses must be developed, completed, and approved for implementation before proceeding with implementation of the original system change.

Refer to Section 6.3 for more information on safety requirements approval and implementation decision-making and signatures.

### 3.7.4 Determining Predicted Residual Risk

**Predicted residual risk** is the risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk reduction have been explored. The predicted residual risk is based on the assumption that controls are in place and/or all safety requirements are implemented and are valid. If safety requirements are not documented in the PHAT, predicted residual risk should be the same as the initial risk.

If the risk cannot be reduced to an acceptable level after attempting all possible risk reduction strategies, either revise the original objectives or abandon the proposed change. If an acceptable proposal is not identified, the change cannot be implemented. Similarly, if a change was implemented without safety requirements and the predicted residual risk was not met, the safety analysis for this project must be revisited in the SMS database’s MOC module, which may require the development of safety requirements. Refer to Section 4.3.2 for more information.

## 4.1 Developing Safety Performance Targets

**Safety performance targets** are measurable goals used to verify the predicted residual risk of a hazard. A safety performance target is the preferred means to relate the performance of risk reduction efforts to the expected risk level. The safety performance target is included as part of the monitoring plan (see Section 4.2).

Safety performance targets are used to assess safety performance with respect to controls and newly implemented safety requirements. Do not define the worst credible effect or effects producing the highest risk level as the safety performance target; instead, look at the less severe effects or indicators (e.g., the number of unauthorized vehicle deviations on taxiways per a specific number of airport operations over a period of time). Safety performance targets should be related to the hazard or system change.

Use subject matter experts to determine the appropriate metrics to monitor when developing safety performance targets. The sources of data used when preparing to assess the system change should be evaluated when developing safety performance targets. The pre–Safety Risk Management committee data analysis serves as the basis for comparison against the post-implementation metrics.

Mapping a hazard to a specific safety performance target may not be possible in terms of establishing a causal relationship. In such cases, identify a sound alternate method to verify the predicted residual risk and determine whether controls and/or safety requirements are appropriate and are functioning as intended.

## 4.2 Developing the Monitoring Plan

The monitoring plan should be comprehensive to verify the predicted residual risk. The monitoring plan includes the safety performance targets or another sound method to verify the predicted residual risk. Create a plan for each hazard that defines:

* Monitoring activities;
* The frequency and duration of tracking monitoring results; and
* How to determine, measure, and analyze any adverse effects on adjoining systems.

### 4.2.1 Monitoring Activities

The monitoring organization must verify that the controls and/or safety requirements were indeed put in place and are functioning as designed. Specifically, this means that procedures must be stringently followed and hardware or software must function within the established design limits.

Detail the methods by which the risk acceptor’s designee will gather the performance data or monitoring results. The organization that accepted the risk is responsible for comparing the monitoring results against the defined safety performance targets or using the results to determine whether predicted residual risk was met. Refer to Section 6.4 for information about risk acceptance.

It is important to retain objective evidence that the safety requirements have been implemented. Objective evidence is simply documented proof. The evidence must not be circumstantial; it must be obtained through observation, measurement, testing, or other means. The most common way of documenting the implementation of safety requirements in the SMS database is through *corrective actions and preventive actions* (CPAs) in the *Issue Manager* module. Use the existing SMS database integration to manage CPAs stemming from:

* Operational process issues;
* Operating environment change issues;
* Audit and assessment findings;
* Accident and incident investigations;
* Non-compliance investigations; and
* Other employee reported issues.

In the SMS database, CPAs belong to:

* reported issues;
* audit findings; and
* Management of Change (MOC) projects.

To monitor CPAs, assign “Next Review Dates” on the Assess tab in Issue Manager for each parent issue. “Next Review Dates” allow automated alerts to be forwarded to managers in charge of tracking activities.

To document monitoring activities, consider the use case:

* For items living in the SMS database’s *Issue Manager* and for audit findings, use the Validate tab to prove that each issue has been reviewed.
* For Management of Change (MOC) projects in the SMS database, for each monitored project, there are two potential areas to document monitoring activities:
  1. Issue Manager’s “Validate” tab for the related action plan; or in the
  2. “Plan for Review/Audit of Actions” section using “Details for Review/Oversight” text box.
* For hazards in PHAT, review the “Predicted Residual Risk” and the “Monitoring Plan.” The risk acceptor’s designee leaves comments in the “Risk Review Comments” section for each reviewed hazard. The responsible manager (risk acceptor” may leave comments in the “Responsible Manager Review” section.

#### 4.2.1.1 Monitoring Operational Processes

Monitoring operational processes is what managers do on a day-to-day basis (e.g., direct supervision of employee activities, monitoring of pilot currency, and monitoring Minimum Equipment List (MEL) status). Monitoring also involves reviewing data that is collected for operational purposes to look for anything of safety significance (e.g., duty logs, crew reports, work cards, process sheets, and reports from the employee confidential reporting system). This may include monitoring products and services from outside sources that are used in the certificate holder’s operations.

Most of the data/information-gathering for monitoring of operational processes will likely occur as a normal business process by the management personnel who are directly involved in the day-to-day operations. For example, regularly reviewing (e.g., weekly, monthly, or quarterly) the flight dispatch logs and crewmember duty records is a form of monitoring and could be conducted during the normal course of duties.

Hazards, non-conformities or other issues detected during monitoring of operational processes will be submitted within 24 hours after detection in the SMS database’s employee confidential reporting system.

#### 4.2.1.2 Monitoring Operational Environment Changes

Monitoring of the operational environment involves practices that are similar to those of monitoring operational processes as described in section 4.2.1.1. The context for monitoring the operational environment of a system is developed from the system analysis (see section 3.3 SRM Phase 1: Describe the System) that is conducted in the SMS database's PHAT module.

Once the scope of the operational environment is defined under SRM, the operational environment must be monitored to assess impacts on aviation safety. For example, increases in the price of fuel may require airlines to change their scheduling, routes, and aircraft utilization.

Hazards, non-conformities or other issues detected during monitoring of operational environment changes will be submitted within 24 hours after detection in the SMS database. The means to report the abnormality to initiate SRM activities includes, but is not limited to:

* Employee confidential reporting system; and
* Proactive Hazard Analysis Tool (PHAT) module.

### 4.2.2 Frequency and Duration of Monitoring

When considering the frequency and duration of tracking monitoring results, account for:

* The complexity of the change,
* The hazard’s initial risk level,
* How often the hazard’s effect is expected to occur (i.e., likelihood),
* Controls,
* Types of safety requirements being implemented (if any), and
* Amount of time needed to verify predicted residual risk.

For example, when considering a hazard associated with the familiarity of a new procedure, a relatively short tracking period would be required until a person or population could reasonably be expected to adapt to the new procedure and the predicted residual risk could be verified. However, the monitoring plan for a hazard associated with new separation criteria may require several years of tracking to verify the predicted residual risk.

## 4.3 Post-SRM Monitoring

It is critical to obtain feedback on key safety performance indicators through continuous monitoring. Organizations responsible for performing Quality Control and/or Quality Assurance use audits and assessments to monitor the safety risk and performance of an implemented change documented in the monitoring plan. The responsible organization determines whether an implemented change is meeting the safety performance targets documented in the monitoring plan.

Results of post-implementation monitoring help determine whether a change remains a validated part of the system or must be reassessed through the Safety Risk Management (SRM) process.

### 4.3.1 Monitoring and Current Risk

A hazard’s current risk is updated at each monitoring interval (in accordance with stated monitoring frequency). Current risk provides an indicator of whether safety requirements are meeting the predicted residual risk. The risk acceptor assesses the current risk as often as prescribed for the duration of the monitoring plan.

Hazard monitoring activity may be verified using the SMS database’s *Hazard Risk Register*. Inspect the “Next Review” date to determine whether any reviews have been skipped or whether a hazard’s review has not been documented properly.

Continuous hazard monitoring may be performed using the SMS database’s Issue Manager. When reported issues and audit findings are classified using associated hazards from the Hazard Risk Register, management has an opportunity to review the respective hazards’ controls and determine whether current risk levels align with actual observations.

### 4.3.2 Predicted Residual Risk Is Not Met

Through monitoring current risk and the safety performance of a recently implemented change, it may become clear that the predicted residual risk is not being met. If this occurs, the safety analysis must be revisited to assess the risk of the new hazards or develop additional safety requirements to lower the risk to an acceptable level. There are several reasons why the predicted residual risk may not be met:

* The safety requirements or controls may not be properly mitigating the risk,
* The initial risk may have been assessed inaccurately,
* Unintended consequences may have occurred, or
* New hazards may be identified.

In either case, the risk acceptor must coordinate a reassessment to determine if changes to the risk management strategy are necessary. An SRM committee must be convened to assess the risk of the new hazards and/or develop additional safety requirements to lower the risk to an acceptable level. Refer to Section 5 for information about SRM committees and Section 6.7 for information on updating safety documentation.

### 4.3.3 Predicted Residual Risk Is Met

The successful completion of monitoring is a prerequisite to hazard and change closeout. This includes the achievement of safety performance targets and/or the predicted residual risk. Safety performance targets for key safety performance indicators are documented in the SMS database’s “*Goals and Objectives*” module.

The monitoring procedures used to verify the predicted residual risk must also be documented in PHAT for each monitored hazard, as they will be used to evaluate the safety performance of the change after it is added to the operation’s system. The established monitoring requirements must be followed, even after meeting the goals of the monitoring plan.

### 4.3.4 Residual Risk

**Residual risk** is the level of risk that has been verified by completing a thorough monitoring plan with achieved measurable safety performance targets. Residual risk is the assessed severity of a hazard’s related consequences (effects) and the frequency of the effect’s occurrence.

To document residual risk assessments, risk assess each hazard related consequence in PHAT during review to support the documentation efforts. If nothing has changed since last review, the risk acceptor simply documents the review activity in the respective “Responsible Manager Review” section.

### 4.3.5 Monitoring and Tracking of Changes Added to System

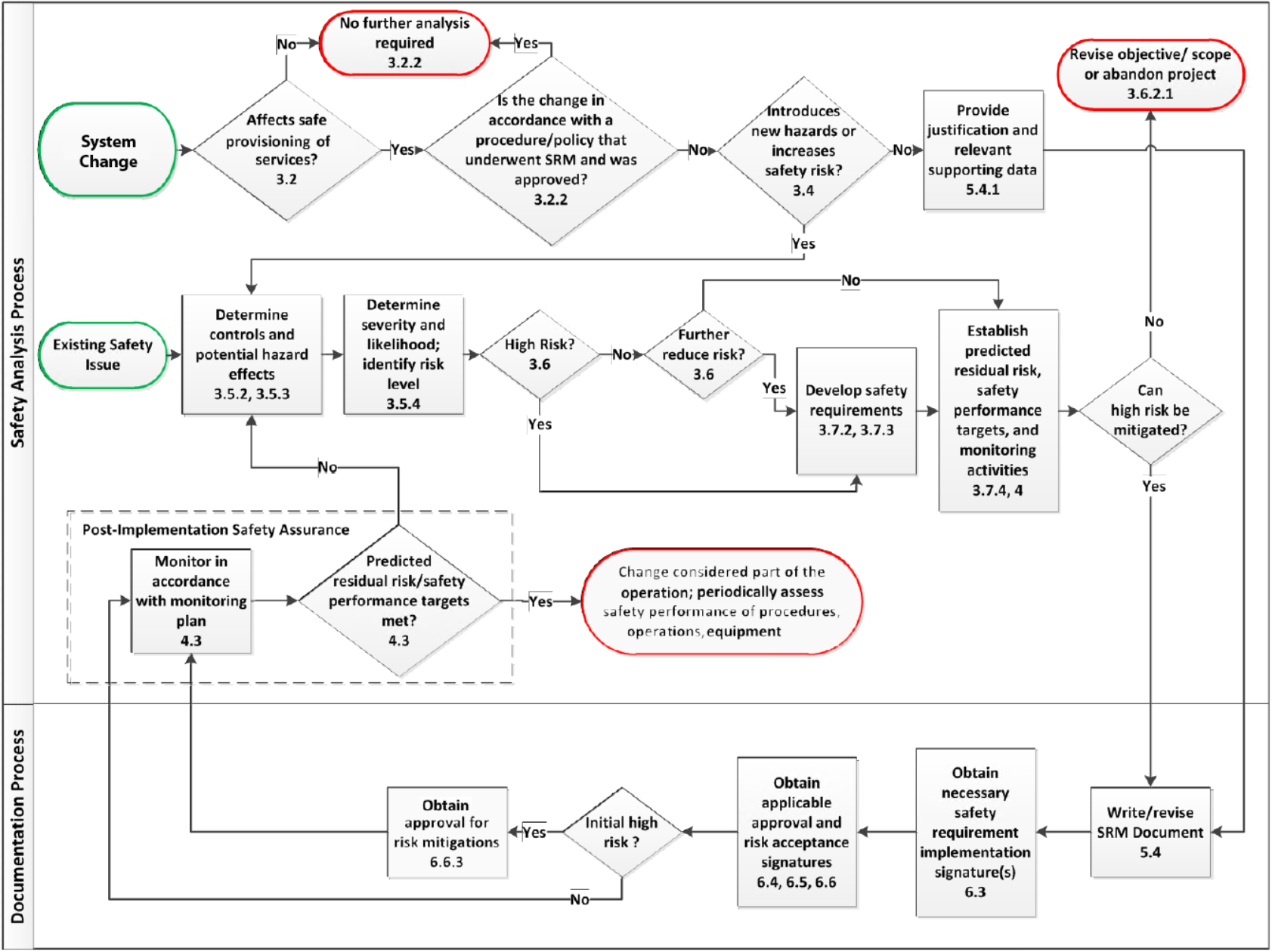
A change is considered completely integrated into the system only after monitoring is completed, the safety performance target is achieved and maintained, and/or the predicted residual risk is verified. At that point, the change is monitored through existing Safety Assurance (SA) processes to determine whether an acceptable level of safety is maintained. The change and all of the associated safety requirements become part of the system, which will become the basis from which all future changes will be measured. If a safety requirement is altered or removed from a change that was made part of the operation’s system, a new SRM analysis must be performed.

The documentation that was developed during the SRM process is critical to SA functions, which often use SRM documents as inputs to assessments and evaluations. The process for preparing, performing, and documenting the safety analysis is described in Section 5.

## 5.1 Safety Analysis Overview

### 5.1.1 Safety Analysis Process Flow

Figure 5.1 depicts the overall process for performing the safety analysis for an existing safety issue or a system change and proceeding through the administrative process for getting the safety analysis and its associated safety requirements through the approval process. The figure separates the safety analysis process from the documentation approval and review process (see Section 6), in which the analysis is recorded in a Management of Change (MOC) Safety Risk Management (SRM) document. Refer to Section 5.4 for additional information on MOC SRM documentation.



**Figure 5.1 Safety Analysis Development and Approval Process**

## 5.2 Preparing a Safety Analysis

### 5.2.1 Planning and Initial Decision-Making

The scope of the Safety Risk Management (SRM) effort is based on the type, complexity, and effect of the change or existing safety issue. It is critical that the level of detail in the safety analysis matches the scope and complexity of the change or existing safety issue (see Section 3.3.2.4). To support this activity, the change proponent should consult his or her Director of Safety, or a local safety point of contact when initiating the process. The following steps are essential to performing any initial decision-making, as well as planning and preparing for a safety assessment of all changes and existing safety issues:

* Clearly define the change or existing safety issue.
* Scope the operational system and/or environment affected.
* Decide the extent to which SRM must be performed and/or documented.
* Coordinate with other organizations that may be affected by the change or the potential risk management strategies.
* Identify an SRM committee facilitator, if necessary.
* Identify a facility/organization/program/technical lead (i.e., a Subject Matter Expert (SME)).
* Identify appropriate SRM committee members by consulting with the SRM committee facilitator.

SRM is needed to address confirmed existing safety issues identified in the system (e.g., Top 5 safety issues and other safety issues identified in corrective action and preventive action (CPA) requests). When addressing existing safety issues, the hazard and its risk level may be pre-determined. It is not necessary to reassess the validity or current risk level of any existing safety issue identified and confirmed by a safety audit or post-event safety risk analysis. The purpose of performing SRM on existing safety issues is to identify safety requirements or other actions to reduce the associated risk to an acceptable level. At minimum, apply SRM to the existing safety issue; however, the risk assessment should also account for the risk impact of any proposed safety requirements.

#### 5.2.1.1 Scope

The change proponent, along with a small group of technical experts, must properly define the purpose and scope of the change (see Section 5.3). The group should follow the guidance and requirements in Section 3.1.1 to determine the impact of the change on relevant equipment, operations, and procedures.

#### 5.2.1.2 Detecting Potential for Hazards

After defining the scope and purpose of the change, the change proponent and a small group of technical experts should determine if there are any potential safety hazards associated with the change or if the change could increase risk associated with equipment, operations, and/or procedures. Review Section 3.4 for assistance in determining the existence of safety hazards associated with the change. When the change does not have potential to affect safe provisioning of services, no further analysis is required. Conversely, if there is potential for the change to affect the safety of the system, the change proponent should proceed to perform an in-depth safety analysis (refer to Section 5.2.2).

### 5.2.2 Preparing for In-Depth Safety Analyses

If the change proponent and initial group of SMEs determine that there are safety hazards associated with a change, a more in-depth safety analysis must be performed. Likewise, when using SRM to address an existing safety issue, a more in-depth approach is warranted. This decision will necessitate a larger group of SMEs and stakeholders, typically called an SRM committee. The role of the SRM committee is to objectively examine potential hazards and effects associated with the change. The SRM committee only assesses the safety of the change, not its suitability, validity, or necessity. SRM committees must not use committee deliberations to define what the change should be or attempt to reassess the purpose or intent of the change defined by the organization(s) sponsoring the change.

#### 5.2.2.1 SRM Committee Facilitator

The change proponent selects or requests an SRM committee facilitator. All SRM committees are led by a facilitator, who is a trained expert in facilitation and SRM. The role of the facilitator is to work with the change proponent to help scope the safety analysis and moderate the deliberations of the SRM committee. The SRM committee facilitator should become well-versed in the subject matter (e.g., by requesting briefings and collecting all available and relevant safety information), as necessary, before the SRM committee convenes. The facilitator will ensure all relevant information about the change or existing safety issue is sent to the SRM committee members before the committee meeting.

An effective SRM committee facilitator ensures the SRM process is followed in an unbiased manner and works to achieve consensus. He or she

* captures the decisions of the committee members,
* mediates any disagreements,
* documents any dissenting opinions, and
* remains neutral throughout the process without advocating for a specific outcome.

The facilitator/co-facilitator (or his or her designee) may write the safety document describing the safety findings of the SRM committee meeting.

#### 5.2.2.2 Facilitation by Safety Case Leads

A safety case lead may facilitate the SRM effort for changes that meet any of the following criteria:

* The change has a high (potentially political, economic, or financial) impact on company operations or stakeholders.
* The change is the result of financial or operational decisions made by executive management.
* The change includes means to reduce any safety risks identified as part of the Top 5 Program.
* The change modifies safety policy that must be incorporated in a directive.
* The change can or does present operational or technical conflicts to multiple affected Lines of Business (LOBs) or company divisions.

#### 5.2.2.3 Pre–SRM committee Assessment of the Scope of the Safety Analysis

After selecting a facilitator, the change proponent and facilitator will have an initial meeting to prepare for the SRM committee. During this time, the facilitator will provide a briefing to the change proponent on the SRM committee. This meeting will be used to define:

* The change or existing safety issue,
* The system state(s) in which the change will be operational,
* Assumptions (not controls) that may influence the analysis, and
* The components of the 5M Model or SHELL Model.

When defining the components of the 5M Model, adhere to the following guidelines:

* **Mission:** There should be agreement on the language for the change or existing safety issue that the SRM committee is tasked to assess. Ensure that the language is unambiguous, concise, and clearly reflective of the change.
* **Human:** Identify stakeholders that are affected by the change or existing safety issue. Firstly, identify organizations that are affected by the change or existing safety issue. Secondly, proceed to identify SMEs from each of those organizations. Be mindful that further discussions may identify the need to add other organizations to the SRM committee. There may be times where it is not feasible to obtain participation from some of the identified stakeholders. In those cases, other avenues of collecting input or data may be used, such as telephone interviews, worksheets, surveys, etc.
* **Machine:** Define the hardware and software involved in the change or existing safety issue.
* **Management:** Define the documents that are relevant to the change or existing safety issue (e.g., directives, policies, Standard Operating Procedures, Letters of Agreement).
* **Media:** Define the elements of the system that are affected by the change or existing safety issue.

Coordination and preparation between the change proponent and facilitator will result in the development of a briefing package to provide to the SRM committee members. The briefing package should include an invitation, an agenda, briefing materials, and location of the meeting. All documents should be shared with the SRM committee members sufficiently in advance of the committee meeting.

SRM committee meetings may be setup and managed in the SMS database’s *Meeting Manager* module. When using Meeting Manager, ensure all SRM committee members are invited and all attachments are included in the meeting invitation. Document meeting minutes on the “Minutes” tab in Meeting Manager and communicate meeting results (publish) within 24 hours after concluding the meeting.

#### 5.2.2.4 SRM Committee Membership

##### 5.2.2.4.1 Overview

The change proponent works closely with the SRM committee facilitator to identify the SRM committee participants necessary to assess the safety of the change. The size and composition of the SRM committee will vary with the type and complexity of the proposed change or current risk. The SRM committee must be limited to an appropriately sized team of stakeholders and SMEs. A stakeholder is considered to be an entity that could be affected by the proposed change from a safety risk perspective (i.e., an entity responsible for any of the following tasks:

* implementing the change when approved,
* accepting the residual risk,
* implementing safety requirements, or
* affirming controls).

##### 5.2.2.4.2 Participation on SRM Committees Outside of a Service Unit or Our Company

Employees are often requested to participate as stakeholders or SMEs on SRM committees sponsored by organizations outside of their Service Unit or our company. It is important to support these requests, regardless of whether they originate within or outside of our company. Participation as an SME or stakeholder does not necessarily mean that the organization represented by an SRM committee member is responsible for developing or implementing safety requirements, accepting risk, or approving the safety analysis. Refer to Section 6 for information on safety requirement approval and implementation, risk acceptance, and documentation approval.

##### 5.2.2.4.3 Primary SRM committee Roles

Any SRM committee meeting attendee should fulfill at least one of the roles specified as follows:

**Change Proponent:** An individual, facility, or organization within the company that is proposing or sponsoring a change or means to address an existing safety issue.

Functional Description: Among other responsibilities, the change proponent works with the SRM committee facilitator to identify stakeholders and the scope of the safety analysis. The change proponent may deem it appropriate to permit SRM committee observers. The change proponent (or his or her designee) may write the safety document describing the safety findings of the SRM committee meeting.

Note: The safety case approver should not be a committee member.

**SRM Committee Facilitator/Co-Facilitator:** A trained expert on the SRM process who moderates the deliberations of the SRM committee members from a neutral position.

Functional Description: Refer to Section 5.2.2.1 for more information.

**SRM Committee Member:** A selected individual who objectively performs the safety assessment using the SRM process.

Functional Description: An SRM committee member is a stakeholder who represents the program, facility, organization, or constituency potentially affected by the safety risk, the safety requirements associated with the proposed change, and/or the existing safety issue.

**Subject Matter Expert:** A technical expert on the change, hardware or software system, or proposed solution undergoing safety assessment.

Functional Description: An SME is typically an organization’s employee; however, when the organization does not have the expertise in-house, a vendor or industry representative may be invited to fulfill the SME role. The SME answers questions from the SRM committee members. An SME does not participate in the safety assessment and his or her consensus on the safety implications is not sought.

Note: In other areas of the Safety Management System Manual, the term “Subject Matter Expert” is used generically. Each SRM committee member is expected to have technical knowledge in a subject area that would suggest his or her participation in the committee meeting is appropriate.

**SRM Committee Observer:** An individual present during the proceedings of the SRM committee meeting.

Functional Description: An observer is someone attempting to gain a better understanding of the SRM process, not the specific change being assessed. He or she is not an active member of the SRM committee meeting, does not provide input during the deliberations, and may not use electronic recording devices during the committee meeting. Committee observers are permitted at the discretion of the change proponent.

##### 5.2.2.4.4 Examples of Skills and Backgrounds for SRM committee Members

The change proponent and SRM committee facilitator should select and involve SRM committee members with varying levels of experience and knowledge to promote a comprehensive and balanced consideration of the safety issue. They should obtain information on the knowledge, experiences, positions, and thoughts of each member. The following list, though not all-inclusive, provides types of experts to consider for participation on an SRM committee:

* Employees directly responsible for developing the change or managing the existing safety issue,
* Employees with current knowledge of and experience with the system or change,
* Hardware/software engineering and/or automation experts (to provide knowledge on equipment performance),
* Human factors specialists,
* Systems specialists,
* System operators,
* Employees skilled in collecting and analyzing hazard and error data and using specialized tools and techniques (e.g., operations research, data, human factors),
* Quality Control / Quality Assurance employees (to help ensure that the safety performance target is measurable and auditable or to help develop an alternate means to verify predicted residual risk),
* Information/cyber-security specialists,
* Third-party stakeholders,
* Maintenance technicians.

The 5M Model or the SHELL Model, described in Section 3.3.3.2, is useful for identifying potential SRM committee members. Note that it may be necessary to elevate a request for participation to an appropriate management level to ensure participation by all affected stakeholders.

## 5.3 Performing a Safety Analysis

Following the identification and invitation of subject matter experts and stakeholders, the Safety Risk Management (SRM) committee is convened. During the SRM committee, the facilitator will lead participants in objectively examining, identifying, and mitigating potential safety hazards and effects associated with the change or existing safety issue.

### 5.3.1 First Day of the SRM Committee

On the first day of the SRM committee meeting, the facilitator or a designee must present an SRM committee orientation that includes:

* A briefing on the agenda for the meeting;
* A summary of the goals and objectives for the SRM committee;
* A brief review of the MOC SRM process;
* SRM committee ground rules;
* Assessment method(s) by which SRM committee will identify hazards (if known); and
* A draft of the “Current System” and “Description of Change” sections of the MOC SRM document, if available, provided by the change proponent (see Section 5.4.3.1).

### 5.3.2 Administering the SRM Committee Meeting

The SRM committee facilitator may perform or delegate the function of time keeper in order to manage start times and breaks. The facilitator may also delegate the recording of meeting minutes, the writing of the MOC SRM document, and the provision of audio/visual support. In some cases, a co-facilitator may assist. A co-facilitator is especially helpful when the committee size exceeds 12 members and/or the subject matter is complex.

The SRM committee should be conducted using in-person meetings, if possible; however, stakeholders can participate in SRM committee meetings via other methods, such as web meetings or teleconferences. In the event that the invited stakeholders cannot participate in an SRM committee, consult with the change proponent and, if feasible, continue the safety assessment as scheduled. The findings should then be forwarded to the absent stakeholders to gather additional input, comments, or concerns.

### 5.3.3 Factors that Jeopardize Safety Assessment Results

Failure to adequately describe the system and scope of the safety analysis can negatively affect the fidelity of the risk analysis and potentially hinder the implementation of a change. Change proponents, facilitators, and SRM committee members should adhere to the following guidelines to help ensure that SRM committee deliberations support the goals of the change proposal:

* Sufficiently define the scope.
* Involve relevant stakeholders.
* Identify drivers and constraints.
* Define product boundaries and external interfaces.
* Baseline the scope before writing requirements.

### 5.3.4 SRM Committee Deliberations

SRM committees should strive to reach consensus, but there may be instances in which not all SRM committee members agree on the results of the safety analysis. In those cases, document the results of the analysis, record the opinions of the dissenters, and deliver the results to the decision-maker. Safety and Technical Training department encourages dissenting SRM committee members to provide their own rationale and data for why their severity and/or likelihood determination differs from that of the other SRM committee participants.

The SRM committee facilitator must mediate and assist SRM committee members in working through differences of opinion. The facilitator should be able to recognize, acknowledge, and use differences of opinion to help the SRM committee consider different points of view.

## 5.4 Documenting a Safety Analysis

### 5.4.1 MOC SRM Documents

A **Management of Change (MOC) Safety Risk Management (SRM) document** is used to record safety analyses for changes, or changes stemming from existing safety issues. The MOC SRM document presents evidence supporting whether the change and/or risk management strategies should be accepted by management officials from a safety risk perspective.

#### 5.4.1.1 Safety Finding with Hazards

MOC SRM documents are used to reflect two types of safety scenarios. The first is a safety finding with hazards. In this scenario, a change or existing safety issue is assessed by an SRM committee, and the committee perceives or determines that hazards could be introduced or that safety risk could increase. When this scenario applies, an in-depth safety analysis is required, which typically results in new means to reduce risk (i.e., safety requirements) being devised and proposed for implementation. Safety risk and overall safety performance is monitored after implementation of the change and/or safety requirements to address the identified hazards. In this case, the entirety of Section 5.4.3 applies.

##### 5.4.1.1.1 Proactive Hazard Analysis Tool

Use the Proactive Hazard Analysis Tool (PHAT) to organize the SRM committee’s deliberations. The PHAT serves as a guide for the hazard and risk analysis. This delineation allows assessments performed across the company to be consistently catalogued and managed.

#### 5.4.1.2 Safety Finding Without Hazards

Alternatively, an SRM committee uses an MOC SRM document to reflect a safety analysis that was performed but did not reveal new hazards or any perceived or calculated increase in safety risk. This is a safety finding without hazards. When this scenario applies, the MOC SRM document should include a description of the system and change and a rationale supporting why the change does not introduce hazards or increase safety risk. Refer to Section 5.4.3 for the full list of required content.

Note: When addressing existing safety issues, the approach for safety findings with hazards (see Section 5.4.1.1) is the most appropriate.

The purpose of SRM is not to record all modifications to elements of the system. SRM documentation should strictly consider and document safety concerns and safety findings. Certain modifications may not necessarily be considered system changes under the purview of this Safety Management System (SMS) Manual. The change proponent must consider potential safety ramifications when making any modification to the system (see [Section 3.2.1)](https://my.faa.gov/org/linebusiness/ato/safety/sms/documents/smsmanual/SMS3_2.pdf).

Modifications that do not relate to safety will not require SRM and do not need to be documented. Contact the Director of Safety for assistance, if necessary.

### 5.4.2 MOC – Management of Change (MOC)

The company SMS database’s MOC module is the official repository for all MOC SRM documents and their safety findings. The SRM committee, change proponent, or organization accepting safety risk must enter the safety analysis and associated documentation into MOC before the initiation of monitoring activities, the completed implementation of the change.

The MOC SRM document sections align with MOC data entry requirements. Refer to Section 5.4.3 for descriptions of applicable items based on MOC SRM documents “if hazards are identified” or “if no hazards are identified.” MOC provides a “PDF Report View” that automatically populates based on safety analysis findings with or without hazards. The information in this view is listed in the order shown in Section 5.4.3.

### 5.4.3 Completing the MOC SRM Document

The change proponent, the SRM committee facilitator, or a designated individual should begin drafting the MOC SRM document during the SRM committee meetings. The collated results of the safety assessment should be presented to the group to verify that the SRM committee members’ discussions have been correctly recorded and concurrence has been achieved. In the event that the SRM committee cannot reach concurrence, those who wish to record a dissent may do so in writing. Such dissents are included in the MOC SRM document for evaluation by the risk acceptance official.

The change proponent, SRM committee facilitator, or designated individual should provide the draft MOC SRM document to the SRM committee for review. He or she must enter the safety assessment into MOC, as per Section 5.4.2.

The following list reflects applicable sections and criteria for MOC SRM documentation in MOC SRM documents. See Section 5.4.3.1 through Section 5.4.3.5 for more information about the content of each SRM document section.

* Executive Summary
  + Administrative Information
  + Reason for Change
  + Details of Change
  + Affected Parties
* System Analysis with Short Description
* New Hazards / Risk Summary (if hazards are identified)
* Rationale for Safety Finding Without Hazards (if no hazards are identified) – Use comments or attachment
* Mitigation
* Management Approval
* Assessors (SRM Committee Attendees)
* Attachments

#### 5.4.3.1 Executive Summary

The Executive Summary provides the substantive information necessary for reviewers and decision-makers to understand the change / existing safety issue, associated safety risk, and the proposed ways to address the hazards and safety risk.

##### 5.4.3.1.1 Administrative Information

* **Title.** Include a clear, concise name of the document with which the document’s subject can be easily understood.
* **Company Project #.** Provide a company project number if initiated from another business unit or use default.
* **Triggering Conditions:** Indicate what initiates/triggers this change
  + Ineffective risk control
  + INFO
  + New destination
  + New operational process/procedure or change to existing
  + New regulatory guidance
  + New system design or change to existing design
  + Operational environment change
  + SAFO (Safety Alerts for Operators)
  + Other

##### 5.4.3.1.2 Reason for Change

Provide a succinct, detailed description of the hardware/software system, operation, or procedure that constitutes the change. Refer to [Section 3.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS3_3.pdf#page=1&zoom=auto,70,720) for information on Phase 1 of the SRM process, “Describe System.” Include the following information when applicable:

* A brief background on what triggered the need for a change or the evaluation of an existing safety issue. If there is an associated safety analysis (from PHAT), reported issue (from Issue Manager), compliance issue (from audit findings), or Top 5 issue (from Executive Dashboard) that necessitated this change, briefly summarize it here and include the associated reference number or documentation as attachments.
* The current hardware or software system or existing procedures/operations and the corresponding (operational) system states.
* The current procedure and its operational environment and, when applicable, a discussion about elements of this issue that make it particularly unique or challenging.
* Equipment or procedures needed to accommodate the implementation of the change.
* Future configuration, system, or procedural changes that might affect the proposed change/procedure or existing safety issue.

##### 5.4.3.1.3 Details of Change

Provide a description of the proposed change or the existing safety issue being addressed. Refer to [Section 3.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS3_3.pdf#page=1&zoom=auto,70,720) for information on Phase 1 of the SRM process. Include the following information when applicable:

* A description of the proposed change/procedure or existing safety issue and any critical safety parameters that are involved (e.g., prohibited/restricted airspace, noise abatement area, operational limitation).
* When applicable, discuss the types of verifications that will be performed throughout the development process to review whether the finalized proposed Change will be safe, operational, and effective once implemented. Evaluation can consist of simulator modeling, live testing, or a combination thereof.
* Assumptions that make evaluating the change or existing safety issue more manageable or that better scope the analysis.
* A summary of the relevant results of any related or preceding safety analyses (i.e., an acquisition program or operational change). Include any references and/or associated documentation mentioned in Section 5.4.3.5.

##### 5.4.3.1.4 New Hazards / Risk Summary (If Hazards Are Identified)

Use this section to include a summary of the findings of the safety analysis and how the SRM committee came to its conclusions. Provide the number of high, medium, or low initial risks associated with the change or existing safety issue. Within this section, include one of each of the following items:

* **Hazard List.** In the MOC section called “Associated Hazards Related to Change,” drag and drop associated hazards from the Hazard classifications to the relevant category (e.g., Environment, Personnel, Equipment, Facilities).
* **Safety Requirements.** For each new hazard, in the MOC “Hazard Identification Analysis” section, indicate for each hazard its identification number, a safety requirement recommended by the SRM committee, and the organization responsible for implementation. A signature from the Point of Contact (POC) responsible for the implementation of each safety requirement must be included in the attachment’s section.The appropriate signatory, not the SRM committee, determines if a safety requirement is planned for implementation. If a safety requirement will not be implemented, the appropriate party must include a rationale in the safety requirement form or as an attachment if additional space is needed (see Section 6.3.2.1). To complete this section, see [Section 3.7](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS3_7.pdf#page=1&zoom=auto,70,720) for information on Phase 5 of the SRM process, “Treat Risk.”
* **Monitoring Plan.** In the MOC section called, “Details for Review/Oversight,” indicate for each hazard its identification number, associated monitoring activities, associated safety performance targets, and the POC responsible for performing the monitoring. See [Section 4](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_1.pdf#page=1&zoom=auto,70,720) for more information.

##### 5.4.3.1.5 Rationale for Safety Finding Without Hazards (If No Hazards Are Identified)

There may be cases in which, through performing elements of the SRM process (i.e., describing the system/change and identifying hazards), hazards associated with the implementation of the change are not identified, or it is determined that the change does not increase the current risk level. In such cases, include a detailed rationale that explains how the SRM committee or team came to that conclusion. When the provisions of this section apply, the MOC is considered complete and should be prepared for collecting signatures (see [Section 6](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_1.pdf#page=1&zoom=auto,70,720) for information on signatures). In all other cases, use the guidance in the remaining sections.

##### 5.4.3.1.6 Mitigation

In the MOC section called “Mitigation,” list the control measures for each related risk, including the control name, owner, status and hierarchy of control. This information should also be configured in PHAT for each related hazard.

##### 5.4.3.1.6 Attachments List

Provide references to any attachments that support the findings of the safety analysis. For more information, see Section 5.4.3.5.

#### 5.4.3.2 Management Approval

Listed below are the approvals required in the MOC details page. For each approval, include the printed name and date. Managers should login to the SRM database software and manage their respective approval sections. Hard-copy signatures may optionally be obtained, and then be listed, in the following order: approver, risk acceptor, and who closed or implemented change (when necessary). Hard copies of signatures can be included as attachments.

1. **Approval.** Include an electronic approval signature from an official representing the organization responsible for implementing the change (and from our company Director of Safety, if required). An approver provides a technical and administrative quality control review of the safety analysis, its findings, and the identified results. Refer to [Section 6.6.](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_6.pdf#page=1&zoom=auto,70,720)
2. **Risk Acceptance.** Include a risk acceptance signature from an appropriate official representing the organization that will be using the safety-assessed equipment, policy, or procedure. This signature indicates acknowledgment of the identified safety risk(s) and denotes its acceptance into the system upon implementation of the Change. Refer to [Section 6.4.](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_4.pdf#page=1&zoom=auto,70,720)

#### 5.4.3.3 Assessors

Include a list of each SRM committee member’s name and relevant information including his or her position, department or facility. Make clear whether he or she participated as a facilitator, subject matter expert, SRM committee observer, SRM committee member, or change proponent. Refer to [Section 5.2.2.5](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS5_2.pdf#page=3&zoom=auto,70,340) for more information.

#### 5.4.3.4 Hazard and Risk Analysis (If Hazards Are Identified)

Documenting hazards in PHAT remains essential to providing an analysis that thoroughly captures and categorizes the hazard. PHAT and the associated hazards’ monitoring plan provide the necessary details to support continuous monitoring of the change through audits and reported issues managed in the SMS database’s *Issue Manager*. Some acquisition analyses/assessments may not require completion of all sections of the *PHAT*.

#### 5.4.3.5 Attachments

Use attachments to include the following:

* Additional or previous safety analyses that are pertinent to the findings in the current analysis undergoing review and approval;
* Supporting documentation such as simulations, modeling, and other technical analyses;
* Required signatures (e.g., approval and risk acceptance),
* Relevant references; and
* Acronyms, terms, and definitions.

### 5.4.4 Implementation Dates in PHAT and Issue Manager

Once the MOC SRM document has been completed and all required signatures have been obtained, the change proponent is responsible for providing a monitoring start date (i.e., the date after all safety requirements are implemented). For related hazards associated with this change, document the monitoring activities in the respective hazards under the “Monitoring Plan” section. The monitoring start date should be entered into Issue Manager’s review date to trigger the automated email notification process for the monitoring plan. Periodic reviews can also be scheduled in Issue Manager on the Assess tab to alert management of monitoring milestones.

## 5.5 Special SRM Efforts/Considerations

Some Safety Risk Management (SRM) efforts may be in response to atypical system changes. Other efforts need to address safety issues or support decisions expediently to circumvent existing policies and processes. While the requirement to perform SRM still applies, management acknowledges the need to truncate, deviate from, or add to the safety analysis process in some cases. In other cases, the requirement for SRM must be reiterated. Use this section for information related to the specific SRM documentation/process requirements and considerations for the following:

* Deactivation, removal, or decommissioning of equipment
* Emergency modifications
* Existing high-risk hazards

### 5.5.1 Deactivation, Removal, or Decommissioning of Equipment

Over time, equipment, procedures, systems, and services must be removed due to limited parts, obsolete services, funding constraints, facility relocation, or a function no longer being needed. If equipment, procedures, systems, or services are removed, discontinued, deactivated, or decommissioned from the company, then a safety risk assessment must be performed in accordance with this Safety Management System (SMS) Manual. The safety risk assessment must be completed before the equipment, procedures, systems, or services are removed from the system. The results of the safety risk assessment must be uploaded to the Management of Change (MOC) database module and hazards updated in PHAT (see Section 5.4.4), and any identified means to reduce risk and safety performance targets must be monitored by the equipment, procedure, system, or service owner.

### 5.5.2 Emergency Modifications

When an emergency modification is necessary, a memorandum must be sent to our company Director of Safety within two days of the implementation of the modification. The memorandum must:

* State what system was modified,
* Provide a summary of the emergency modification,
* Identify why the modification was made, and
* Indicate when the safety risk assessment will be conducted.

The department head who authorized the emergency modification must ensure that a safety risk assessment is performed in accordance with this SMS Manual within 30 days of the implementation of the modification. After the safety assessment is completed, a follow-up memorandum must be sent to our company Director of Safety stating that the safety assessment has been completed and uploaded to MOC and related hazards in PHAT have been updated. Our company Director of Safety must inform our company Accountable Executive (AE).

### 5.5.3 Existing High-Risk Hazards

When an existing hazard is determined to be a high-risk hazard, our company Director of Safety must notify our company’s AE and system department heads of the high risk and any interim actions to mitigate the risk. Our company AE must either approve the interim action and accept the associated risk or require that the operation be stopped.

Thirty days after the notification is sent to the AE and department heads, the responsible department head must coordinate with our company Director of Safety to develop a permanent plan that will eliminate the hazard or reduce the risk to an acceptable level and provide that plan to the safety and technical training officer. The plan must include:

* Description of hazard and system state,
* Severity and likelihood of the high risk,
* Data or empirical evidence that justifies the determination that a high-risk hazard exists,
* Safety requirements or a decision to cease the operation,
* Schedule to complete an MOC SRM document in accordance with this SMS Manual, and
* An approval signature by each department head of responsible/affected departments.

Cessation is viable if the prescribed means are inadequate to reduce the risk to an acceptable level. In some cases, though, cessation of the operation may not be the safest means to mitigate the risk. There could be unintended consequences that result in more potential harm or increase system safety risk.

The affected department must forward the plan with a memorandum via its Department Head to the safety and technical training Department Head for approval and copy our company Director of Safety, who will then forward the memorandum to our CAA point of contact. The safety and technical training department will notify our CAA’s point of contact of any subsequent changes to the approved plan.

The hazard must be documented in the MOC database module that is written in accordance with this SMS Manual and uploaded to PHAT within 30 calendar days of the implementation of the final safety requirements. The responsible department must adhere to the MOC SRM documentation approval and risk acceptance requirements documented in this SMS Manual. Refer to Section 6.3 for information on the review and approval of the MOC SRM documentation.

## 6.1 Risk Acceptance and Approval and Overview

The review and approval of Management of Change (MOC) Safety Risk Management (SRM) documents and acceptance of any safety risk is designed to maintain and assure the quality of risk management activities. There are key variables that affect safety risk acceptance and MOC SRM documentation review and signature requirements. They include

* the organization(s) affected by the proposed system change,
* the organization that developed the document,
* the risk(s) associated with the Change, and
* whether the Change is considered system-wide or local in scope.

There are several signature authorities associated with MOC SRM documentation: approval, risk acceptance, and safety requirements implementation. Refer to [Section 6.2](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_2.pdf#page=1&zoom=auto,70,720) for information regarding system-wide and locally scoped changes.

For guidance on specific signature types, refer to [Sections 6.3](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_3.pdf#page=1&zoom=auto,70,720) through [6.6.](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_6.pdf#page=1&zoom=auto,70,720) Tables 6.1 through

6.4 summarize the MOC SRM document signature requirements. The terms “affected facilities” and “affected Service Units” refer to the facilities or organizations that are impacted by the safety risk associated with the Change or existing safety issue.

Note: Table 6.1 is not to be used for safety analyses with an unacceptable (high) predicted residual risk (see Table 6.4).

**Table 6.1 Signatures for MOC Approval and Risk Acceptance**

**(Use with Section 5.4.1.1, Safety Findings with Hazards)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of Change** | **Requires CAA Approval/Acceptance?** | **Initial Predicted Risk Level** | **Required MOC/SRM Acceptance Signatures** | **Required MOC/SRM Approval Signatures** |
| Local | No | Low/Medium | Department Head of affected department(s) | Director of Safety |
| Yes | Low/Medium | Department Head of affected department(s), Director of Safety | Director of Safety |
| High | Department Head of affected department(s), Director of Safety | Department Head of affected department(s), Director of Safety, Accountable Executive |
| System-wide | Yes/No | Low/Medium | Department Heads of affected department(s) | Director of Safety |
| High | Department Head of affected department(s), Director of Safety | Director of Safety, Accountable Executive |

Notes:

(1) The change proponent must ensure that MOC SRM documents are entered into our company MOC database module for tracking and monitoring the status of Changes.

(2) Signature responsibility may only be delegated from an Accountable Executive to a Department Head.

(3) The changes that require CAA approval are listed in [“enter location where required changes are listed.”](https://employees.faa.gov/tools_resources/orders_notices/index.cfm/go/document.information/documentID/14251) If there is an initially identified high-risk hazard, the CAA must approve the means to reduce safety risk and the Director of Operations and our company Director of Safety (8) must sign the document.

(4) The proponent of a system change must send an informational copy of the SRM document to the Department Head of affected service area before submitting the SRM document to our company Director of Safety for approval.

(5) In cases where medium or low safety risk and/or controls go outside of our company, the mitigations must be approved by the designated management officials within the other Lines of Business (LOBs) and accepted by the CAA.

(7) Our company Director of Safety must submit safety cases with means to reduce safety risk of any initially identified high-risk safety hazards to the CAA for approval.

(8) If the change or existing safety issue meets the criteria for CAA approval, our company Director of Safety must submit it to the CAA accordingly.

(9) Risk acceptance must be obtained for safety analyses in which risk is identified, except for the Operational Safety Assessment and the Comparative Safety Assessment.

(10) For approval and/or risk acceptance outside of our company, the CAA may facilitate signatures on behalf of our company. However, the Service Unit change proponent should obtain signatures from the affected organization (user) participating on the SRM committee.

(11) Re-engineering changes should start with Table 6.2 for their signature requirements.

**Table 6.2 Signatures for Re-engineering MOC Approval and Risk Acceptance**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Proposed Modification to Approved System-Level Requirements?** | **Does Previous Safety Assessment Document Safety Implications of Proposed Change?** | **Facilitated by Safety & Training Department or Requires CAA Approval or Acceptance?** | **Hazard Identified?** | **Required MOC Approval Signatures** | **Required Safety Risk Acceptance Signatures** |
| No | Yes | No additional assessment required | | | |
| No | No | Yes | Upper Management | Department Head of affected department |
| No | Upper Management | None |
| Yes | Yes | See signatures required in Table 6.1 | |
| No | Upper Management | None |
| Yes | Yes/No | Yes | Yes | See signatures required in Table 6.1 | |
| No | Upper Management, Director of Safety | None |
| No | Yes | See signatures required in Table 6.1 | |
| No | Upper Management, Director of Safety | None |

Notes:

(1) This table applies to system-wide Changes only. For local changes, refer to Table

6.1. Refer to [Section 6.2](https://my.faa.gov/content/dam/myfaa/org/linebusiness/ato/safety/sms/documents/ATO-SMS-Manual/SMS6_2.pdf#page=1&zoom=auto,70,720) for a discussion on system-wide and local-level Changes.

(2) The change proponent must ensure that the MOC hazards are entered into PHAT for tracking and monitoring the status of Changes.

(3) Signature responsibility may only be delegated from an Accountable Executive to a Department Head.

(4) System Level Requirements refer to the requirements listed in accepted PHAT hazards or in other approved system documentation.

(6) In cases where medium or low safety risk and/or controls go outside of our company, the means to reduce safety risk must be approved by the designated management officials within the other business units and accepted by the CAA.

(7) Our company Director of Safety must submit the means to reduce safety risk of any initially identified high-risk safety hazards to the CAA for approval.

**Table 6.3: Signatures for MOC/SRM Approval (Use with Section 5.4.1.2, Safety Finding Without Hazards)**

|  |  |
| --- | --- |
| **Type of Change** | **Required MOC/SRM Approval Signatures** |
| Local | Department Head of affected department(s), Director of Safety |
| System-wide | Accountable Executive, Director of Safety |
| Acquisitions | Department Head of affected department(s), Director of Safety |

Notes:

(1) The change proponent must ensure that the MOC SRM document is entered into PHAT for tracking and monitoring the status of Changes.

(2) Signature responsibility may only be delegated from a Accountable Executive to a Department Head.

(3) For local changes, the MOC SRM document is signed one level above the Department Head at the facility completing the MOC SRM document.

**Table 6.4: Signatures for MOC/SRM Approval for Proposed Changes Only (Use with safety analyses with unacceptable [high] predicted residual risk)**

|  |  |
| --- | --- |
| **Type of Change** | **Required MOC/SRM Approval Signatures** |
| Local | Department Head of affected department(s), Director of Safety |
| System-wide | Accountable Executive, Director of Safety |

Notes:

(1) When the predicted residual risk is unacceptable (high), CAA approval is not required.

(2) Per Safety Management System policy, a high predicted residual risk is unacceptable and the Change in question must not be implemented. The MOC submitter is responsible for notating this in MOC module and closing out the safety analysis.

(3) Signature responsibility may only be delegated from an Accountable Executive to a Department Head.

## 6.2 Scope of Changes

System changes are considered either local or system-wide. A system-wide Change is one for which a safety case lead facilitates or leads the Safety Risk Management (SRM) effort or that meets at least one of the following criteria:

* The Change has high visibility or a potential political, economic, or financial impact to the company or our clients
* The Change is the result of financial or operational decisions made by upper management
* The Change includes means to reduce any safety risk identified as part of the Top 5 Program.
* The Change modifies safety policy that must be incorporated into standing procedures.
* The Change could or does present operational or technical conflicts to multiple affected Service Units.
* The Change will be implemented on a company-wide level, affecting either multiple facilities or the entire company.

Note: There may be cases in which a safety case lead facilitates a local SRM committee and none of the aforementioned criteria apply. These changes will be considered local.

A Change is considered to be local if:

* It does not meet any of the preceding criteria and it affects a single Service Area or
* It is a change proposed by operations involving a single piece of equipment that is restricted to one area of operations.

### 6.2.1 Local Implementation of System-Wide Changes

When the local implementation of a system-wide scoped MOC SRM document cannot follow the company standard, local SRM is required to assess and accept any risk for local deviations. If formal waivers are required in such cases, local SRM does not eliminate the waiver requirement.

## 6.3 Approving Safety Requirements

An organization’s safety requirement approval signature represents its commitment to implementing the safety requirements in accordance with the associated Management of Change (MOC) SRM document.

### 6.3.1 Appropriate Signatories

Safety requirement signature authority must be at the managerial level with the ability to fund and ensure the implementation of the safety requirement. The appropriate signing official may be determined by the accountable executive. When multiple officials are responsible for providing safety requirements signatures in an MOC SRM document, they must share similar managerial status or responsibility.

When an organization outside of the company is responsible for a safety requirement, a signature on file is required. This requirement may be met through a memorandum or an MOC SRM document. The change proponent is responsible for following up on the status of the implementation of safety requirements identified in the MOC SRM document.

### 6.3.2 Endorsing Implementation of Safety Requirements

All safety requirements that the SRM committee identifies must be accounted for in the MOC module and Proactive Hazard Analysis Tool (PHAT). The change proponent and appropriate safety requirement(s) POCs must collaborate to determine which safety requirements will be implemented and notate that decision in PHAT and in the MOC’s SRM document.

Only safety requirements that are to be implemented must have an accompanying signature. Refer to Section 6.3.2.2.

#### 6.3.2.1 Safety Requirements Not Planned for Implementation

If a safety requirement is not going to be implemented:

1. The rationale for not implementing the safety requirement must be entered in the MOC SRM document on the safety requirements form and recorded in PHAT. In addition, if any of the SRM committee members dissent with the removal of the safety requirement, the dissention must be recorded in the MOC either as an attachment or in the “Remarks” section.
2. The panel must be contacted to verify that the predicted residual risk, safety performance target, and/or monitoring plan have not been impacted.

If the predicted residual risk, safety performance target, and/or monitoring plan must be changed as a result a safety requirement not being planned for implementation, the SRM committee’s revised analysis must be documented, along with any dissenting opinions.

#### 6.3.2.2 Safety Requirements Planned for Implementation

All safety requirements included in the Hazard Identification Analysis section of the signed MOC SRM document must be implemented before or in conjunction with the system change, even when the risk is classified as medium or low. All organizations responsible for implementing a safety requirement must:

1. Sign the MOC SRM document for the safety requirement approval,
2. Document the status of the safety requirement (e.g., implemented, not implemented, or in progress), and
3. Record objective evidence supporting the safety requirement’s implementation.

#### 6.3.2.3 Safety Recommendations

Safety recommendations may be uploaded to their respective MOC project as attachments to the MOC SRM document. They do not require any endorsement.

## 6.4 Risk Acceptance

Risk acceptance is certification by the appropriate management official that he or she acknowledges and accepts the safety risk that is expected to remain once the system change is fully implemented. Safety risk must be accepted before the implementation of a proposed Change and the execution of the monitoring plan. Risk acceptance is based on the predicted residual risk (see Section 3.7.4). Risk acceptance and other inputs (e.g., cost-benefit analysis) are necessary before a change to the system can be implemented. When an individual or organization accepts a risk, it does not mean that the risk is eliminated; some level of risk will remain.

Risk acceptance requires:

* Signed confirmation from the appropriate management official that he or she understands and accepts the predicted residual safety risk(s) associated with the hazard(s) identified in the safety analysis;
* Signatures for the safety requirements identified in the Management of Change (MOC) Safety Risk Management (SRM) document;
* Approval of the safety performance target(s) or alternate method(s) identified to verify the predicted residual risk associated with each hazard, confirming that the safety performance target(s) or identified alternate method(s) can be used to measure the current risk; and
* A comprehensive monitoring plan that the risk acceptor agrees to follow to verify the predicted residual risk.

For system-wide implemented Changes, risk can be accepted by upper management. However, if a department is not able to comply with all of the safety requirements or has additional hazards and/or causes that were not identified in the system-wide MOC SRM document, a local assessment must be completed (with local risk acceptance) prior to the implementation of the Change. Refer to Section 6.2.1 for information on local versus system-wide implementation of safety requirements.

### 6.4.1 Authority to Accept Safety Risk

The acceptance of the safety risk depends on the span of the program or Change and the associated risk. In most cases, the responsibility for risk acceptance ultimately lies with the department(s) affected by the Change. Risk acceptance authority also depends on whether a Change is local or system-wide in scope.

### 6.4.2 Risk Acceptance Outside of our Company

If the affected party is outside of the company (e.g., navigation or weather services), each department responsible for establishing requirements for contracted services accepts the risk into the system. Organizations outside of our company may also be responsible for components of the system and have a role in accepting safety risk.

Directors, managers, and supervisors must work closely with their counterparts in organizations outside of our company to help ensure that the appropriate party or parties accept and manage any safety risk resulting from Changes. Again, it is not in compliance with company policy to implement a Change without having accepted any associated safety risk.

## 6.5 MOC SRM Document Approval

Approval of a Management of Change (MOC) Safety Risk Management (SRM) Document with Hazards requires and represents that:

* The MOC SRM document was developed properly,
* Hazards were systematically identified,
* Risk was appropriately assessed,
* Valid safety requirements were proposed for unacceptable risk,
* Safety performance targets or other methods to verify predicted residual risk were approved by the responsible Service Unit, and
* An implementation and monitoring plan was prepared.

**Approval of an SRM Document without Hazards** requires and represents that:

* The MOC SRM document was developed properly,
* No hazards were introduced by the change,
* The analysis did not address an existing safety issue,
* The Change will not affect risk, and
* Sufficient justification exists to support the no-hazards finding.

In approving MOC SRM documentation, the approval authority affirms that the aforementioned items have been performed and agrees that the underlying assumptions are reasonable and the findings are complete and accurate. MOC SRM documentation approval does not constitute approval for implementation or acceptance of any risk associated with the Change or existing safety issue.

### 6.5.1 Department MOC SRM Documentation Approval

Affected or stakeholder Service Units (departments) must assign an appropriate management official to provide approval of the safety analysis. The person selected must be available to provide input to the management official(s) who will accept the risk associated with the Change or existing safety issue.

If MOC SRM documentation must be sent outside of the Service Unit for approval (e.g., to another Service Unit or the safety and technical training department), the documentation must have an approval signature before it leaves the Service Unit. All identified means to reduce safety risk requiring approval and acceptance by the CAA must first be sent through the safety and technical training department.

If MOC SRM documentation requires the approval of more than one Service Unit, discrepancies in the approval standards or processes may exist between the departments. In these cases, the change proponent should request that safety and technical training department adjudicate the discrepancies.

If a safety and technical training department safety case lead managed the development of a safety analysis / MOC SRM document (see Section 5.2.2.2), the MOC SRM documentation does not require department approval; however, the department(s) responsible for accepting the risk must still review and sign the MOC SRM document before the Change can be implemented. If a safety case lead develops the MOC SRM document, the relevant/affected operational department(s) that accepted the associated risks of the Change or existing safety issue must follow the monitoring plan documented in the MOC SRM document.

### 6.5.2 Safety and Technical Training Department Review and Approval

Safety and technical training department review and approval is a technical and non-technical assessment by safety and technical training department safety case leads to verify that the MOC SRM process has been followed, that the safety documentation is complete, and that the safety documentation adheres to the Safety Management System (SMS) Manual principles and guidelines.

Any documentation forwarded to the external organizations for approval must first go through a safety and technical training department peer review. For a safety and technical training department peer review, forward MOC SRM documentation to the safety case lead in draft form and without signatures. At this point, the safety case lead will facilitate the remaining steps in the review process. When the MOC SRM document is ready for signature, the safety case lead will notify the change proponent, who will obtain the appropriate signatures. Finally, when the MOC SRM document has all signatures except for that of our company Director of Safety, the safety case lead will present the MOC SRM document to our company Director of Safety for signature. Other MOC SRM document requirements (see Section 5.4.3.2) that are documented in this SMS Manual remain.

### 6.5.3 Coordination of MOC SRM Documentation

Safety and technical training department will collaborate with the CAA to obtain the necessary reviews, approval, and risk acceptance signatures for MOC SRM documentation with all applicable organizations outside of our company for all Changes. The scope of potential changes includes products, services, systems, and procedures associated with external facilities. Service Unit change proponents may initiate these reviews and signatures through outside organizations. However, the Service Unit change proponent must inform the appropriate safety and technical training department safety case lead of such action.

## 7.1 Audit and Assessment Programs

### 7.1.1 Overview

Safety and technical training department’s Safety Assurance programs evaluate compliance with Safety Management System (SMS) requirements and Civil Aviation Authority (CAA) orders, standards, policies, and directives. Audit and assessment programs evaluate:

* Effectiveness of performance and operations in the Service Units,
* Effectiveness of internal Quality Control efforts (e.g., operational skills assessment, system service review, certification, periodic maintenance, modification, and availability),
* Effectiveness of Quality Control mitigation efforts in response to identified trends and risks,
* Trends identified from safety data analysis,
* Effectiveness of safety-related policies and procedures, and
* Compliance with SMS requirements.

### 7.1.2 Difference between Facility Audits and Assessments

The department head of each operational area conducts internal compliance verifications of his or her operational area. Safety and technical training department conducts audits based on identified or suspected safety issues and non-compliance. The department determines priorities by soliciting input from other company departments and by analyzing objective criteria from sources such as occurrence reports, *Hazard Risk Register* in SMS database, and risk analysis results. In addition, Safety and technical training department conducts no-notice spot inspections of facilities and operational activities.

### 7.1.3 Independent Assessments

Safety and technical training department performs independent assessments to evaluate operational procedures, order compliance, fielded systems, and safety benefits. A safety and technical training department independent assessment is independent of department responsible for the assessed program or operation. Independent assessments are post-implementation evaluations of Changes that assess actual performance.

During independent assessments, the teams verify that any previously documented hazards were rated accurately (based on observed data) and that no unacceptable safety risks exist. In addition, teams may identify operational issues and other findings.

Independent assessments may involve:

* several related assessments over a long period of time,
* one assessment that lasts for an extended period of time, or
* multiple brief assessments.

The processes and procedures for an independent assessment are tailored according to its duration and the complexity of the operation or program being assessed. The assessment may be conducted at one or multiple sites, and data may be collected on site or remotely. Results and/or recommendations are based on the assessment team’s analysis of data collected during and, if applicable, before the assessment. The conclusions and recommendations are independent from external sources.

## 7.2 Safety Data Reporting, Tracking, and Analysis

Safety Management Systems (SMSs) require the collection and analysis of data from different sources and various vantage points to determine if hazards exist. The key to safety data analysis is developing the capability to sort and analyze a vast array of data and transform the data into information that permits the identification and mitigation of hazards, preventing future incidents and accidents.

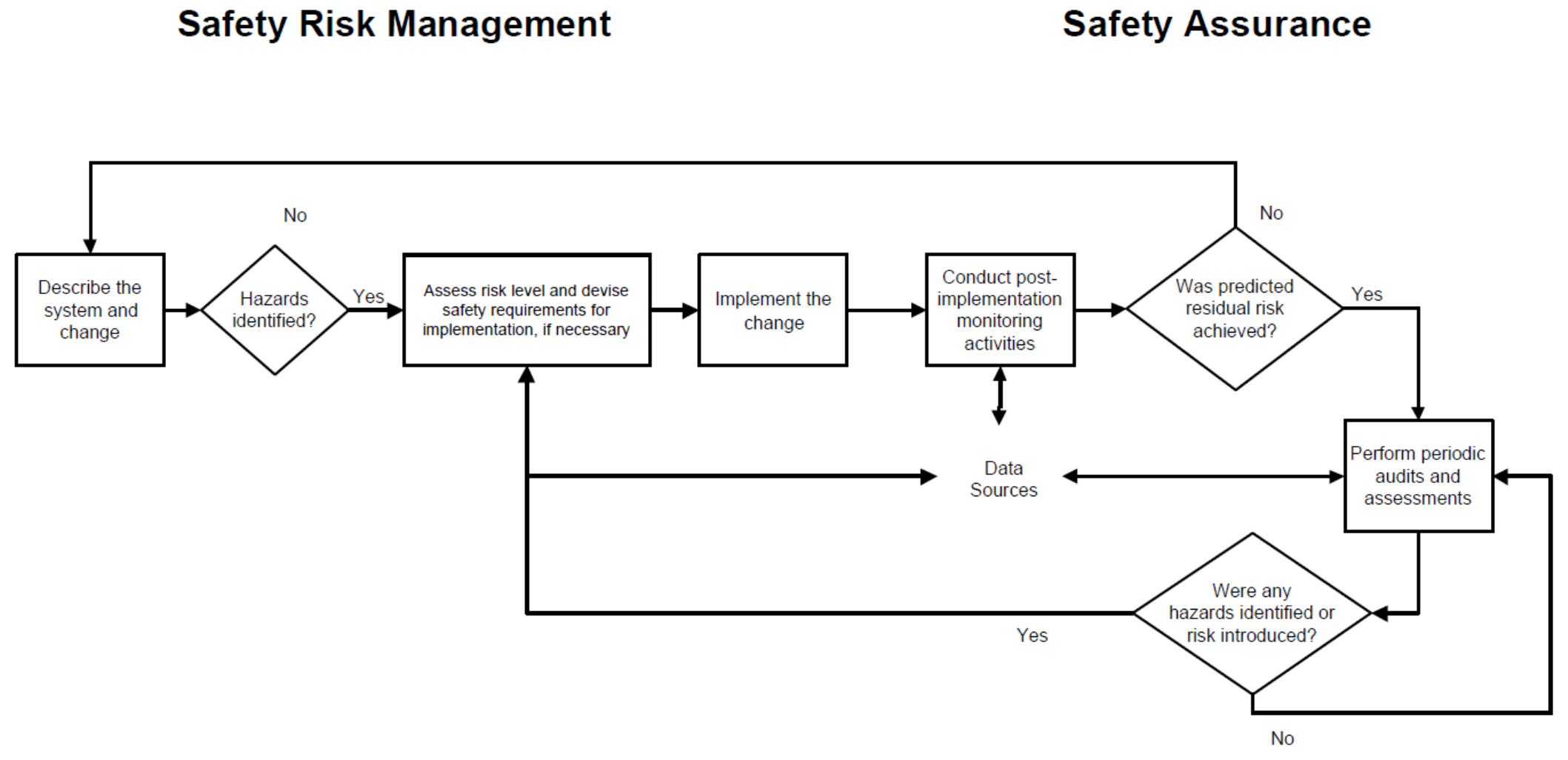
### 7.2.1 Purpose of Safety Data Collection and Evaluation

The tracking and analyzing of safety data to enhance operational awareness of potentially hazardous situations is a critical aspect of the SMS. Safety and technical training department assists with the collection and analysis of company-wide and division-specific safety data and supports sharing the data to continually improve the safety of the company’s system.

Safety data are used to:

* Identify risks, trends, and vulnerabilities in the system;
* Determine the effects of a Change on the operation as a whole;
* Assess the performance of safety requirements in managing risk;
* Identify areas where safety could be improved;
* Contribute to accident and incident prevention; and
* Assess the effectiveness of training.

In most cases, if the analysis of safety data leads to the identification of issues or hazards, the resolution or corrective action constitutes a Change, which may require Management of Change (MOC) Safety Risk Management (SRM). This is an example of the continuous, closed-loop process for managing safety risk. Figure 7.1 depicts the closed-loop process between SRM and Safety Assurance (SA).



**Figure 7.1: SRM and Safety Assurance Closed-Loop Process**

### 7.2.2 Safety and Training Department’s Role in Safety Data Collection and Evaluation

Safety and technical training department obtains safety data through various sources within and outside the system. Safety and technical training department assesses safety by tracking safety metrics to produce reports on system safety, which are shared with appropriate departments and/or external stakeholders.

### 7.2.3 Safety Data Collection and Reporting Processes

The company collects and reports on safety data from various sources in the system. Section 8 lists many of the existing processes, tools and databases related to safety data collection and reporting.

Our company’s non-punitive, voluntary reporting program allows all stakeholders to report an incident or event without reprisal. This program includes integration with the FAA’s Aviation Safety Action Program (ASAP) and the Aviation Safety Reporting System (ASRS). They are designed to foster consistent reporting and higher quality data.

Other mechanisms employed by our company for employees to report issues include email, the SMS database’s Offline Hazard Reporting Tool and the “Public Issue Reporting” modules.

## 7.3 Safety Incident and Accident Reporting and Analysis

Evidence has shown that for every accident, there are many precursor events. Therefore, accident prevention programs focus on the collection, analysis, and investigation of incident data. Incident investigation is valuable because real-world occurrences are analyzed to prevent or eliminate future occurrences. Our company fine-tunes incident prevention measures by analyzing low-level indicators that may contribute to an incident or accident.

Incident reporting prompts our company to conduct investigations. Company employees who conduct the investigations reconstruct and analyze the event. They identify causal factors (also known as contributing factors) and categorize them using a root cause schema. They also review factors that may have lessened the effect of the occurrence, such as documented controls.

Company employees use the information gained from an investigation as input to recommend risk mitigation strategies and safety-enhancing measures to preclude similar events in the future.

Corrective actions and preventive actions (CPAs) can enhance safety at all levels, from system-wide to local. They can include:

* Facility improvements,
* Additional communication, navigation, and surveillance systems and/or automation systems,
* Additional staffing,
* Training; or
* Other safety-enhancing changes.

### 7.3.1 Delegating Risk Management Tasks

The SMS Safety Manager is responsible for ensuring each reported issue is:

* Valid;
* Not a duplicate report;
* Branched to work independently in other divisions (if necessary);
* Issued to the appropriate division or business unit;
* Risk assessed;
* Assigned a due date (targeted closure date);
* Classified by "Type of Issue" and by hazards from Hazard Register; and
* Assigned to the proper Responsible Manager (risk acceptor).

These tasks will be done within 24 hours upon receiving notification of a new issue report via e-mail. Validity, branching and division assignment need to be done before an issue is risk assessed.

Some issues belong to more than one division – these must be branched to all appropriate divisions. When an issue is branched or the division is changed, there is no automated e-mail advisory. The person branching the issue or changing the division must advise the SMS Safety Manager of that division of the change that has occurred. In many cases, this may be the same person, which requires no documented notification.

An issue must be risk assessed and assigned a due date (desired target closure date based on policy) before it can be classified. Initial risk assessments and desired closure dates alert responsible managers of reported issues’ severity and how much time they may have to treat the issue, such as assigning and managing corrective actions and preventive actions (CPAs).

The Responsible Manager assigned to each issue must belong to the division to which the issue is assigned and have "risk acceptance" authority. Some responsible managers have permissions to work within multiple divisions and subsequently must be given a “Shared Division” role, which allows the SMS database to grant access to issues in other divisions.

SMS documentation activities to record mitigations may be performed by a data entry specialist in the SMS database; however, the preferred approach is to have each department head manage their own documentation.

#### 7.3.1.1 Determining Validity of Reported Issues

The SMS Safety Manager will take steps to determine the validity of reported issues when they are received.

Validity is about truth, correctness, relevancy and factual reporting. Reported issues that fail this validity test will be rejected. The reason for rejection will be documented in the reported issue and the report closed. Reported issues that are beyond the scope of SMS may be deleted. Deleted issues may be reviewed by management in the SMS database's *Custom Report Viewer*.

When an original reporter disagrees with the issue's validity, they may submit their complaint and reasoning to the Safety Committee for review at their next regular meeting.

If the safety committee agrees with the SMS Safety Manager, the issue will remain closed. If they disagree, the issue will be re-opened, the reason(s) for re-opening documented, and the issue will be dealt with as per normal procedures.

Validated reports will be dealt with in accordance to the SMS database’s Issue Management Process documented in the SMS database's *Issue Manager* module's Help section.

#### 7.3.1.2 Risk Assessing Reported Issues (Prioritizing Risk)

Each valid reported safety issue will be assigned a priority based on the hazard risk assessment.

A risk statement must be developed, and a risk assessment completed. This will be done by the SMS Safety Manager. The SMS Safety Manager is responsible for initial risk assessments, but risk assessments may be performed with input from relevant parties: assigned responsible manager, safety committee, or subject matter experts (SMEs).

Proof that the responsible manager is reading the Assessment and concurs with the assessment may be obtained by requesting "Receipt acknowledgement requested" notice in the email notification. When the responsible manager acknowledges the receipt of the reported issue assignment without reservations, it is assumed the responsible manager concurs with the initial risk assessment.

Initial risk assessments must be done right away. Risk assessments have top priority because the risk assessment determines the necessary response time (deadline for closure) for any reported issue and related CPAs.

Refer to 3.5.4 Defining Risk for details on risk assessment definitions.

Refer to 3.6 SRM Phase 4: Assess Risk for details on using the risk matrix to assess risk.

#### 7.3.1.3 Maximum Deadline Closure Dates for Reported Issues

* Unacceptable (red): 1 day
* Mitigatable (yellow): 7 days
* Acceptable (green): 30 days (no CPAs required)

#### 7.3.1.4 Generic Action Plan Based on Risk Assessments

**Unacceptable risk (red)**: All work must stop. The situation must be analyzed for root cause(s) and a corrective action plan:

* devised,
* approved by the department head with risk acceptance authority; and
* implemented before resumption of activity.

All appropriate documentation must be completed (i.e. Incident report form, accident report form, injury report form, hazard investigation form, corrective action plan, etc.). If not already done, the report must be entered in the SMS database. Any immediate corrective/preventive action must also be documented in the respective reported issue within the SMS database. All closed issues assessed at this level will be reviewed at the next scheduled safety committee meeting.

Open, “in progress” issues that have been assessed as “unacceptable” may also be included in the next scheduled safety committee; however, the chances are slim they will be included due to the brief required response period.

**Mitigatable (yellow)**: Work can continue, but only after the Responsible Manager (Dept Head with risk acceptance authority) is advised and has reviewed the situation. If not already done, the report must be entered in the SMS database. Any immediate corrective/preventive action must also be documented in the respective reported issue within the SMS database. All closed issues assessed at this level will be reviewed at the next scheduled safety committee meeting.

**Acceptable (green)**: Work can continue. If not already done, the event must be reported in the SMS database, documented as to facts of the safety hazard, and any steps taken to control or eliminate the hazard. Because the risk is low and acceptable, these issues do not require review or validation but these can be done.

#### 7.3.1.5 Investigation of Hazard Reports and Audit Findings

Most issues, whether they are reported issues, internal audit findings, or external audit findings, will be investigated by using the standard SMS Pro processes without opening a detailed, formal investigation. A formal investigation opened in the *Issue Manager's* Investigate tab is not always required.

When the SMS Safety Manager classifies a reported issue or audit finding in Issue Manager's Classify tab, an investigation may be triggered depending upon how the safety team has configured the respective issue’s chosen classification parameters. The determination for formal investigations is set on *Issue Manager's* Classify tab for each respective classification parameter configuration. An issue's subsequent classifications alerts management of the formal investigation requirement.

The Director of Safety determines whether particular classification parameters will trigger formal investigations. This determination shall be made with input from managers with risk acceptance authority.

For example, if an issue involves failure of compliance, an investigation will be triggered when it is classified as such, as long as the classification is configured accordingly. Injuries often require an investigation, but not always. Minor first aid issues are not investigated. A CAA report, where we are mentioned, but not involved, will not require an investigation, whereas one where we are at cause, will be.

##### 7.3.1.5.1 When Investigations Are Required

When investigations are required, a competent person shall be assigned to carry out the investigation by the Responsible Manager assigned to the reported issue or audit finding. An SMS Safety Manager may initiate required investigations whenever reported issue or audit finding classifications determine an investigation is required per policy.

Competent persons managing investigations will have received training in

* Investigation techniques,
* Root cause analysis,
* Risk management, and
* Corrective action planning processes.

Investigation team members may include:

* Safety committee members,
* SMS Admins,
* Company SMS Safety Managers,
* Quality Assurance personnel,
* Other department heads; and
* Subject matter experts (SMEs).

Investigations will be documented in the investigation module of the SMS database, specifically in *Issue Manager’s* Investigate tab. Attachments should be uploaded when required to ensure all investigation documentation resides in one location. The investigation process in the SMS database will be used to determine:

* Sequence of events;
* Root cause analysis; and
* Suitability of proposed corrective and preventive actions (CPAs).

The 5-Why Work-sheet may also be used to determine root cause and may be documented directly in the SMS database on the *Issue Manager’s* **Investigate** tab or alternatively, on the *Issue Manager’s* **Manage** tab.

If another process is used to determine root cause the investigator must

* Attach (upload) the form/tool/worksheet,
* Enter a note indicating the other process used, and
* Explain how root cause was determined.

Note: Root cause classifications in the SMS database require a contributing factor (also known as causal factor). Define required investigation causal factors in the SMS database's *Issue Manager* Investigate tab. Each defined causal factor should be reviewed to determine which root cause classification(s) aligns to each respective causal factor.

The aim of the investigation is to:

* Determine the root cause(s) of the safety hazard, issue or audit finding
* Achieve a safe resolution to the problem (corrective action plan and action).

Note: Investigation results are available to the safety committees through their SMS Safety Manager.

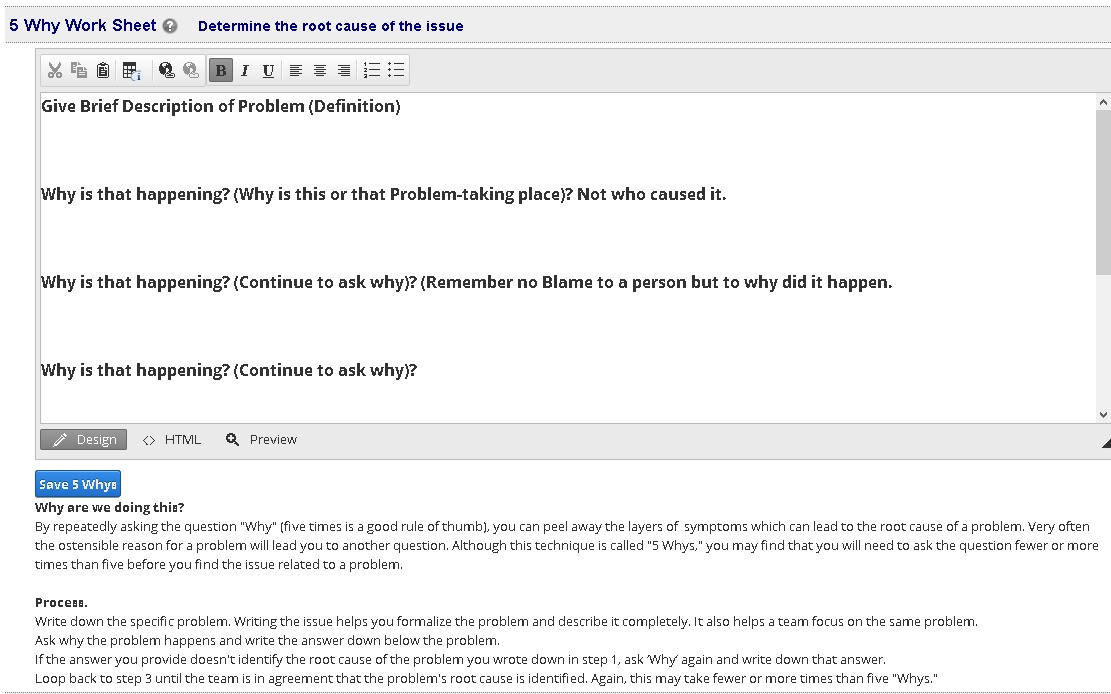
The person(s) investigating shall:

* Discover the facts
* Determine root cause(s)
* Look for possible trends
* Advise the responsible division manager of the results of the investigation.

##### 7.3.1.5.2 When Investigations May Not Be Required

When an investigation is not required, a 5-why analysis may be sufficient to determine root cause. The 5-Why Worksheet form is embedded in the SMS database's Issue Manager module on the "Manage" tab. See Figure 7.2.

**Figure 7.2 5-Why Worksheet in SMS Database**



When not conducting formal investigations in the SMS database, SMS Pro allows for root cause classifications to be documented in the Issue Manager's Classify tab.

Note: As described in section *7.3.1.5.1 When Investigations Are Required*, root cause classifications require a contributing factor (also known as causal factor). Normally, causal factors are defined in formal investigations within the SMS database's *Issue Manager* Investigate tab. A **data-disconnect challenge** arises when classifying root causes outside of the Investigate tab since each defined causal factor becomes associated with an appropriate root cause classification. In these cases, a default "Environmental Exposure" causal factor may be seen on the Investigate tab should a formal investigation be initiated after performing a root cause analysis on the *Issue Manager's* Classify tab. The logic is that the company would not have the particular issue if they were not "exposed to the operating environment," hence the "Environmental Exposure" placeholder.

When a formal investigation (on Investigate tab) is not used to determine root cause, root cause classifications must be conducted using the utility on the Issue Manager's Classify tab.

There are no limitations from stopping the safety or quality team from conducting investigations on issues not requiring formal investigations to investigate the issue and determine root cause using the Investigate tab. Although an investigation may not be required, the Responsible Manager may choose to do one at any time before the issue is closed.

##### 7.3.1.5.3 Starting Investigations on Previously Closed Issues

Whenever formal investigations are warranted for a closed issue, the respective issue’s status must be re-opened, as the issue is no longer considered closed.

##### 7.3.1.5.4 Investigations Not Required for Recent Classification Changes

As discussed in Section 7.3.1.5, the Director of Safety determines which classicization parameters may initiate formal investigations whenever the classification parameter is associated with an issue.

Classification parameters and their related configurations change over time as our company responds to environmental and changes and evolving business requirements. When classification parameters are configured to trigger a required investigation, these new configuration properties will only apply to issues that are not closed.

### 7.3.2 Corrective and Preventive Action Management

Each reported issue must be assigned a responsible manager in the SMS database. By default, the “Default Safety Manager” for each division is assigned the reported issue when it enters the system. “Default Safety Managers” are configured in the SMS database’s Setup >> Customize Settings module.

The responsible manager (Dept Head) has risk acceptance authority and is assigned to manage corrective actions and preventive actions (CPAs) once the safety team has:

* Reviewed the issue;
* Performed an initial risk assessment; and
* Determined the suitable deadline to close the issue (Targeted Closure Date).

Only the assigned responsible manager may accept CPAs and delegate them to either:

* Company employees;
* Vendors managed in the SMS database’s Vendors module; or
* Another third party (vendor or contractor not in the SMS database).

CPAs may be recommended, but not accepted by:

* The reporting user;
* An auditor conducting the audit and making a finding determination;
* A safety team member; or
* Another Dept Head.

There may be times when an assigned responsible manager is unable to manage the reported issue in a timely manner. Another Department Head with risk acceptance authority in the affected area of operations may manage the reported issue’s CPAs.

Some Department Heads have administrative staff available with “Data Entry” permissions in our SMS database. These Data Entry personnel are authorized to document risk management activities in the SMS database; however, the assigned Dept Head always remains accountable for all risk management efforts under his area of operations.

CPAs must have due dates and be assigned to only one person who will be responsible for notifying the responsible manager of the CPA completion. CPA deadlines must be considered carefully. In most cases, CPA deadlines are set before the respective issue’s due date (Targeted Closure Date). Reported issues must have maximum deadline closure dates set based upon the level of risk. See Section 7.3.1.3.

SMS Safety Managers are responsible for monitoring our company’s reported issues and ensuring Responsible Managers are managing their issue(s) for completion within the Maximum Targeted Closure date. When all accepted CPAs have been completed in the SMS database, safety managers are automatically notified by email to take the next steps, which will be to validate that the documentation requirements of the issue have been fulfilled.

Whenever reported issues or audit findings in the SMS database are closed on a date exceeding the defined Targeted Closure Date, the SMS database identifies that item as being closed late. This negatively affects company performance statistics for on-time issue closure that can be found on the SMS database’s Executive Dashboard module. In reality, issues may have been closed before the Maximum Targeted Closure date, but not documented in a timely manner. Therefore, it is important that the safety team documents issues in a timely fashion to avoid confusing responsiveness statistics.

When reported issues are not closed within the Targeted Closure Date, the SMS database displays a warning bell in the Issue Manager's list of open issues. Each day an overdue-issue advisory e-mail is sent to SMS Admins, SMS Executives, SMS Safety Managers, and the respective Responsible Managers to warn of overdue issues. The same business process applies to overdue CPAs and audit findings.

Overdue items are also displayed prominently in the SMS database’s Safety Workspace module. Employees are responsible for managing their assigned items from within their personalized Safety Workspace.

### 7.3.3 Closing Reported Issues, Findings and Setting Review Dates

Once the issue's risk assessment, classification, CPA management and investigation (when required) are completed, a review date (follow-up) may be entered to automatically alert the safety team of the future review. Any member of the safety team may perform the closing risk assessment and then close the issue.

A closing risk assessment must be made. Presumably the risk should be lower after mitigation (this may not always be the case, as it may remain the same depending on the original assessment.)

When closing a report, the safety team should set a future review date. Issues with both low initial and low closing risk assessments do not require review dates; however, there is nothing preventing a future review.

An SMS Safety Manager will periodically review (monthly) recently closed reports to ensure that report documentation is complete and the analysis remains sound.

### 7.3.4 Closing Feedback Loop with Reported Issue Submitter

Employees with user accounts reporting issues in the SMS database have the option to be notified when changes are made to their reported issue and when the report is closed. The SMS database also allows users access to any report they submitted in their personalized "Safety Workspace."

When issue reporters are not satisfied with the actions taken to manage their reported issues, they can refer their report to the appropriate safety manager. They may also enter comments for their reported issue on the Details tab of *Issue Manager*.

Outside sources reporting issues must also be advised of the result of any investigation (both formal and informal), if they provided a name and an e-mail to contact them when they filed their report through the SMS database's *Public Issue Reporting* module.

### 7.3.5 Safety Committee Review of Hazard Reports

Safety Committees, as appropriate, can review Hazard Reports pertinent to their area of responsibilities at their regular meetings. Reports that are risk assessed as "Acceptable" can, but do not need to, be reviewed by safety committees.

In addition, safety committees can be called to an emergency session to review any Unacceptable or Mitigatable assessed reported issues and recommend solutions.

Acceptable hazards that are not resolved at the time of safety committee regular meetings can also be reviewed by another appropriate committee and recommendations for solution proposed at these meetings. The assigned Responsible Manager will take these recommendations into account when determining the corrective action plan.

Safety Managers are required to perform an initial risk assessment and set a tentative “Targeted Closure Date” before scheduling Safety Committee Review. During the Safety Committee Review, the safety committee may discuss the initial risk assessment and modify the assessment and resulting Targeted Closure Date when necessary.

### 7.3.6 Validating Reported Issues and Audit Findings

Issue Validation(review) of each reported issue or audit finding must be completed to determine the effectiveness of the implemented CPAs. The first validation must be scheduled within 180 days of the closing date of the report. Issues that have been risk assessed as "Acceptable" do not require validation.

This Issue Validation (follow-up review) will be done by the assigned Responsible Manager for the issue. When the responsible manager is not available to perform the review, another Department Head with risk acceptance authority in the respective area of operations may conduct the review. Issue validations (follow-up) are done on the Issue Manager's Validate tab.

## 7.4 Reported Safety Data about Serviceability of Equipment, Systems, and Facilities

Significant event reports, and general maintenance logs capture the majority of daily system performance metrics, including incidents. Employees make additional reports in our online SMS database used for accident and incident reporting.

The company’s safety program requires written documentation and management involvement in the review, mitigation, and analysis of trends. Using the company SMS database, personnel conduct periodic independent technical reviews of services provided by systems, sub-systems, and equipment. These reviews also address how well the services match customer needs. Employees are routinely encouraged to file reports on identified deficiencies in the safety or efficiency of procedures, equipment, working environment operations, or services. These notifications may be in the form of:

* Direct email messages;
* Electronic “Message Board” postings; and/or
* Newsletters.

## 7.5 Voluntary Data Reporting

The processes listed above describe the reporting of specific types of safety data. However, over and above the reporting of these data, it is important that each employee reports any occurrence or situation that he or she thinks is or could become a hazard within the system. A positive safety culture depends on this type of voluntary reporting. Our company has formal mechanisms for employees to report issues, including the online Hazard Reporting module in the SMS database. Other reporting systems and SMS tools are listed in Section 8.

**7.5.1 Aviation Safety Action Program (ASAP)**

In cooperation with its employee labor organizations, our company has established voluntary safety reporting programs for pilots and maintenance employees. They allow employees to voluntarily identify and report safety and operational concerns as part of the CAA’s overall safety goals. The collected information is reviewed and analyzed to facilitate early detection and improved awareness of operational deficiencies and adverse trends.

The primary purpose of ASAP is to identify safety events and implement skill enhancements and system-wide corrective actions to reduce the opportunity for safety to be compromised. Information obtained from ASAP will provide stakeholders a mechanism to identify actual and potential risks throughout the system. The programs foster a voluntary, cooperative, non-punitive environment for open reporting of safety concerns. ASAP reports allow all parties to access valuable safety information that may otherwise be unavailable.

Reports submitted through ASAP are brought to an Event Review Committee which reviews and analyzes the submitted reports, determines whether reports require further investigation, and identifies actual or potential problems from the information contained in the reports and proposed solutions. All Event Review Committee determinations are made by consensus. The Event Review Committee may direct skill enhancement or system corrective action and is responsible for follow-up to determine that the assigned actions are completed in a satisfactory manner. Safety Risk Management may be required for corrective actions and preventive actions (CPAs).

## 8.1 Safety Data Gathering and Review Overview

Employees populate several aviation safety databases with information regarding company safety events and serviceability. Many professionals use aviation safety data and information as input for the development of system safety enhancements. Sources for gathering and analyzing safety data and information include:

* CAA recommendations,
* Compliance issues,
* The Risk Analysis Process,
* Requirements for new communication, navigation, surveillance, and automation services;
* Unsatisfactory Condition Reports,
* Employee suggestions,
* Applications for procedural changes (MOC),
* Research and development,
* Acquisition of new systems and equipment,
* Industry advocacy,
* The Safety Risk Management process documented in the Safety Management System Manual, and
* SMS Database.

Table 8.1 provides an overview of various safety tools in and modules in the SMS database.

**Table 8.1 SMS Database Modules**

|  |  |
| --- | --- |
| Name | Short Description |
| Hazard Reporting | Allows stakeholders to report incidents, accidents and irregularities to management. |
| Executive Dashboard | Over 40 miniature dashboard reports to personalize each user’s dashboard. Granular security protects sensitive reports from specified user groups. |
| Safety Workspace | User’s personal workspace to see their SMS activities and follow up without requiring additional resources from the safety team. |
| FRAT | Allows managers to control risk based on individual mission risk assessments. |
| Public Issue Reporting | Allows users outside the company to securely report hazards into the SMS database without having user accounts. |
| Employee Performance Monitor | Employees and managers can see their SMS performance. Managers can review employee performance and set a “Safety Plan” for each employee. |
| Policy & Procedures | Post and manage policies and procedures online for all employees to review. Alerts management when items require review. |
| Duties & Responsibilities | Communicate clearly to stakeholders the duties and requirements of key safety personnel. Employees can acknowledge they understand these requirements. |
| Goals & Objectives | Goals and objectives are communicated to the entire organization using configurable tables and charts. |
| Organization Chart | Organization Chart clearly communicates reporting lines of management structure. |
| Applicable Regulations | List of hyper-links of applicable regulations that the operator must obey. |
| Documents Manager | Online document manager to store SMS documents. Complete with version control and email notifications. |
| ERP | Documents actions employees take immediately following an emergency situation. Manage call lists and document necessary steps to take (e.g. checklists) for different types of emergencies. |
| Issue Manager | Conduct risk assessments, classify issues, manage corrective actions, conduct investigations, and more. |
| Proactive Hazard Analysis Tool | Allows the organization to document hazard identification, associated risks and determine control and recovery measures proactively. |
| Hazard Risk Register | Displays hazard and risk register generated from an Operational Risk Profile in PHAT. Reports of Top Hazards and evaluates controls. |
| Management of Change | Request, manage and document change for SRM activities. |
| CPA Manager | Allows safety managers to monitor corrective actions progress in a single view and easily identify bottlenecks. |
| Risk Analysis Charts | Managers easily review reported issues and identify areas to focus risk management efforts. |
| Risk Impact Trending Charts | Show changes in one or more Y variables over time according to multiple classification types. |
| Customer Report Viewer | Over 20 predefined reports. Filter, sort and export to MS Excel or pdf |
| Classification Report | Generate ad hoc reports and filter issues by classification types, dates, KPIs and much more. |
| Data Analysis & Export | Offers management a way of investigating data and exporting to various formats. |
| Gap Analysis | Conduct a gap analysis against any of multiple models to determine initial gaps and to monitor continuous improvement. |
| Implementation Manager | Used to plan and manage SMS implementation. Configurable implementation plans based on industry models. |
| Auditing | Complete audit suite. Create checklists, schedule audits, conduct audits, track corrective actions and generate reports. |
| Training & Qualifications | Provides a means for operators to manage employee training, qualifications and ratings requirements. |
| Risk Exposure | Monitor’s risk exposure over time by risk severity and number of reported issues. |
| KPI Trend Monitor | Compare key performance indicators (KPIs) against others performance. Trend occurrence reports using statistical analysis. |
| Vendors | Manage vendors or suppliers. Provide ratings, conduct assessments or relate occurrence reports to vendors or contractors. |
| Continuous Improvement | Many chart reports to monitor SMS progress and evaluate problem areas. |
| AE Report | Accountable executive report showing activity based on new items, overdue items and items coming due. |
| SMS Induction | Proves/documents employees understand their SMS roles and documents initial and recurrent SMS training. |
| All Employee Letter | Letter to employees announcing what is SMS and company SMS implementation details. Used for initial SMS training. |
| Meeting Manager | Easily create agendas, invite attendees and document meetings to meet ICAO requirements. |
| Message Board | Provides communications from managers, safety managers, and department heads to all personnel quickly and easily. |
| Training Article Library | Training article repository. Add and assign training resources to employees based on user roles. Used for recurring training activities. |
| Safety Survey | Receive feedback from users about the effectiveness of the SMS. Create and conduct surveys. Instant results. |
| Newsletters | Develop an email-based newsletter for your organization to address trending safety management topics. |
| Lessons Learn Library | Allows users to search for and review past lessons learned from mistakes. Lessons learned generated in Issue Manager investigations. |
| General Issue Viewer | Allows users to view desensitized reported issues and conduct their own analysis. |
| MSDS | MSDS Repository to share MSDS sheets with your organization or others. |

## 9.1 Part 5 FAA Required SMS Processes and Procedures

The FAA Aviation Safety Organization issued a final rule that was published on January 8, 2015, requiring operators authorized to conduct operations under part 121 to develop and implement a Safety Management System. The rule adds a new part 5 to title 14 of the Code of Federal Regulations (CFR), creating the general framework for an SMS that a part 121 air carrier may adapt to fit the needs of its operation. 13 required processes come directly from Part 5 and are described below.

**Safety Attributes** (or process attributes), are inherent characteristics of a system and apply to an effective SMS. The following process attributes must have safety requirements built in to their design if they are to result in improved safety outcomes. To align with FAA’s Safety Management System (SMS) Framework, Revision 3, the following safety attributes are used to describe the required processes.

* Responsibility;
* Authority;
* Procedures;
* Controls;
* Process Measures; and
* Interfaces.

### 9.1.1 Identify Hazards

§ 5.53 System analysis and hazard identification. (c) The certificate holder must develop and maintain processes to identify hazards within the context of the system analysis.

Refer to 3.4 SRM Phase 2: Identify Hazards

### 9.1.2 Analyze Safety Risk

§ 5.55 Safety risk assessment and control. (a) The certificate holder must develop and maintain processes to analyze safety risk associated with the hazards identified in § 5.53(c).

Refer to 3.5 SRM Phase 3: Analyze Risk

### 9.1.3 Conducting Risk Assessments

§ 5.55 Safety risk assessment and control. (b) The certificate holder must define a process for conducting risk assessment that allows for the determination of acceptable safety risk.

Refer to 3.6 SRM Phase 4: Assess Risk

### 9.1.4 Developing Safety Risk Controls

§ 5.55 Safety risk assessment and control. (c) The certificate holder must develop and maintain processes to develop safety risk controls that are necessary as a result of the safety risk assessment process under paragraph (b) of this section.

Refer to 3.7 SRM Phase 5: Treat Risk

### 9.1.5 Acquiring Data to Monitor Operational Processes

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (1) Monitoring of operational processes.

Refer to 4.2 Developing the Monitoring Plan

### 9.1.6 Acquiring Data to Monitor Operational Environments

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (2) Monitoring of the operational environment to detect changes.

Refer to 4.2 Developing the Monitoring Plan

### 9.1.7 Auditing Operational Processes and Systems

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (3) Auditing of operational processes and **systems.**

Refer to 7.1 Audit and Assessment Programs

### 9.1.8 Evaluating SMS and Operational Processes

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (4) Evaluations of the SMS and operational processes and systems.

Refer to 7.1 Audit and Assessment Programs

### 9.1.9 Investigation of Incidents and Accidents

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (5) Investigations of incidents and accidents.

Refer to 7.3.1.5 Investigation of Hazard Reports and Audit Findings

### 9.1.10 Investigating Potential Non-compliance Reports

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (6) Investigations of reports regarding potential non-compliance with regulatory standards or other safety risk controls established by the certificate holder through the safety risk management process established in subpart B of this part.

Refer to 7.3.1.5 Investigation of Hazard Reports and Audit Findings

### 9.1.11 Confidential Employee Reporting System

§ 5.71 Safety performance monitoring and measurement. (a) The certificate holder must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following: (7) A confidential employee reporting system in which employees can report hazards, issues, concerns, occurrences, incidents, as well as propose solutions and safety improvements.

Refer to 1.5.1.1 Employee Confidential Reporting System

### 9.1.12 Analyzing Safety Data

§ 5.71 Safety performance monitoring and measurement. (b) The certificate holder must develop and maintain processes that analyze the data acquired through the processes and systems identified under paragraph (a) of this section and any other relevant data with respect to its operations, products, and services.

Refer to 7.3.1.5 Investigation of Hazard Reports and Audit Findings

### 9.1.13 Correcting Safety Performance Deficiencies

§ 5.75 Continuous improvement. The certificate holder must establish and implement processes to correct safety performance deficiencies identified in the assessments conducted under § 5.73.

Refer to 7.3.2 Corrective and Preventive Action Management

## 10.1 Definitions

**Acceptable Level of Safety Risk.** Medium or low safety risk.

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

**Active Failure.** An error of omission or commission that is made in the course of a particular operation. An active failure can also be a known problem or a known mechanical deficiency or fault.

**Assessment.** A process of measuring or judging the value or level of something.

**Assumptions.** Characteristics or requirements of a system or system state that are neither validated nor verified but are taken as such.

**Audit.** A review of an organization’s safety programs or initiatives to verify completion of tasks and determine an organization’s compliance with CAA directives and procedures.

**Baseline.** The written processes, procedures, specifications, and other conditions of the system that were accepted as the starting point for formally managing safety in the system. Our company must maintain the system at a safety level that is at least equal to that state, in compliance with current policies, processes, and procedures that are documented in its manuals. (Note: “Acceptance of the baseline did not imply or state that the company was or was not inherently safe as configured on that date, nor did it imply that the system had no existing high risks)

**Bounding**. A process of limiting the analysis of the Change or system to only the elements that affect or interact with each other to accomplish the central function.

**Cause**. The origin of a hazard.

**Change.** A modification to any element of the system that pertains to, or could affect the provision flight-related services.

**Change Proponent.** The individual or department within the company that is proposing or sponsoring a Change or means to address an identified existing safety issue. The Safety Risk Management (SRM) panel members are selected at the discretion of the change proponent and/or SRM committee facilitator.

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

**Compliance Audit.** An audit that evaluates or assesses conformance to established criteria, processes, and work practices. The objective of a compliance audit is to determine if employees and processes have followed established policies and procedures.

**Continuous Loop.** SRM processes are repeated until the safety risk associated with each hazard is acceptable and has met its predicted residual risk.

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

**Confirmation.** The act of using a written response from a third party to confirm the integrity of a specific item or assertion.

**Control.** Safety Risk Control: A means to reduce or eliminate the effects of hazards.

**Credible.** It is reasonable to expect that the assumed combination of conditions that define the system state will occur within the operational lifetime of a typical system.

**Critical System.** A system that provides functions or services that, if lost, would prevent users of the system from exercising safe separation and control over aircraft.

**Current Risk.** The predicted severity and likelihood at the current time.

**Development Assurance.** All the planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable approval or certification basis.

**Effect.** The real or credible harmful outcome that has occurred or can be expected if the hazard occurs in the defined system state.

**Equipment.** A complete assembly—operating either independently or within a system/sub­system—that performs a specific function.

**Error-Tolerant System.** A system that is designed and implemented in such a way that, to the maximum extent possible, errors and equipment failures do not result in an incident or accident. An error-tolerant design is the human equivalent of a fault-tolerant design.

**Facility.** Generally, any installation of equipment designated to aid in the navigation, communication, or control of air traffic. Specifically, the term denotes the total electronic equipment, power generation, or distribution systems and any structure used to house, support, and/or protect these equipment and systems. A facility may include a number of systems, sub­systems, and equipment.

**Fail Operational.** A system designed such that if it sustains a fault, it still provides a subset of its specified behavior.

**Fail Safe.** A system designed such that if it fails, it fails in a way that will cause no harm to other devices or present a danger to personnel.

**Fault Tolerance.** The ability of a system to respond without interruption or loss of capabilities in the event of an unexpected hardware or software failure.

**Frequency.** An expression of how often a given effect occurs.

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

**Hazard Identification.** The determination of the hazard scenarios and associated consequences (undesired events) as a consequence of introducing a new system into the system. This provides an intermediate product that expresses the hazards that will be used during risk analysis.

**High-Risk Hazard.** A hazard with an unacceptable level of safety risk; the Change cannot be implemented unless the hazard’s associated risk is mitigated and reduced to medium or low.

**Human-Centered.** The structured process during concept and requirement definition, design, development, and implementation that identifies the user as the focal point of the effort for which procedures, equipment, facilities, and other components serve to support human capabilities and compensate for human limitations; sometimes also called “user-centered.”

**Human Factors.** A multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to equipment, systems, facilities, procedures, jobs, environments, training, staffing, and personnel management for safe, comfortable, and effective human performance.

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

**Initial Risk.** The predicted severity and likelihood of a hazard’s effect or outcomes when it is first identified and assessed; includes the effects of preexisting risk controls in the current environment. Regarding change management, it describes the risk before any proposed mitigations are implemented.

**Inquiry.** The technique of asking questions and recording responses.

**Inspection.** The act of critically examining documents to determine the content and quality of a transaction, such as inspecting leases, contracts, meeting minutes, requirements, and organization policy.

**Latent Failure.** An error or failure whose adverse consequences may lie dormant within a system for a long time, becoming evident when combined with other factors.

**Likelihood.** The estimated probability or frequency, in quantitative or qualitative terms, of a hazard’s effect or outcome.

**Maintenance.** Any repair, adaptation, upgrade, or modification of equipment or facilities. This includes preventive maintenance.

**Management of Change (MOC).** Change management process that identify changes within the organization which may affect established processes, procedures, products and services.

**Management Strategy.** Actions designed to reduce or manage the risk associated with a Change or operation.

**Mitigation.** Any means to reduce the risk of a hazard.

**Objective Evidence.** Documented proof; the evidence must not be circumstantial and must be obtained through observation, measurement, test, or other means.

**Observation.** The process of witnessing an organization’s process. It differs from a physical examination in that the auditor only observes the process; no physical evidence is obtained.

**Operational Assessments.** An assessment to address the effectiveness and efficiency of the organization. The objective of an operational assessment is to determine the organization’s ability to achieve its goals and accomplish its mission.

**Oversight.** Supervision to validate the development of a defined system and verify compliance to a pre-defined set of standards.

**Physical Examination.** The act of gathering physical evidence. It is a substantive test involving the counting, inspecting, gathering, and inventorying of physical and tangible assets, such as cash, plants, equipment, and parameters.

**Preconditions.** The system states or variables that must exist for a hazard or an accident to occur in an error-tolerant system.

**Predicted Residual Risk.** The risk that is estimated to exist after the safety requirements are implemented, or after all avenues of risk mitigation have been explored.

**Preliminary Hazard List (PHL).** A pre-defined list of hazards in the Proactive Hazard Analysis Tool (PHAT). List of potential hazards in the overall operation’s risk profile. Fine-tuning the PHL typically begins with a brainstorming session among the individuals performing the safety analysis.

**Proactive Hazard Analysis Tool (PHAT).** SMS database module designed to categorize and document safety risk management (SRM) activities. PHAT is integrated in Hazard Register, Management of Change, and Issue Manager modules.

**Process.** A set of interrelated or interacting activities that transforms inputs into outputs.

**Qualitative Data.** Subjective data that is expressed as a measure of quality; nominal data.

**Quality Assurance.** A program for the systematic monitoring and evaluation of the various aspects of a project, service, or facility to ensure that standards of quality are being met. It is a process to assess and review the processes and systems that are used to provide outputs (whether services or products) and to identify risks and trends that can be used to improve these systems and processes.

**Quality Control.** A process that assesses the output (whether a product or service) of a particular process or function and identifies any deficiencies or problems that need to be addressed.

**Quantitative Data.** Objective data expressed as a quantity, number, or amount, allowing for a more rational analysis and substantiation of findings.

**Recording.** The process of documenting the identified hazards and the associated safety analysis information.

**Redundancy.** A design attribute in a system that ensures duplication or repetition of elements to provide alternative functional channels in case of failure. Redundancy allows the service to be provided by more than one path to maximize the availability of the service.

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

**Residual Risk.** The remaining predicted severity and likelihood that exist after all selected risk control techniques have been implemented.

**Risk.** The composite of predicted severity and likelihood of the potential effect of a hazard.

**Risk Acceptance.** The confirmation by the appropriate management official that he or she understands the safety risk associated with the Change and that he or she accepts that safety risk into the system. Risk acceptance requires that signatures have been obtained for the safety requirements identified in the SRM document and that a comprehensive monitoring plan has been developed and will be followed to verify the predicted residual risk.

**Risk Analysis Event.** A loss of standard separation between two aircraft in a radar environment that results in less than 66 percent of the applicable separation minima maintained.

**Risk Assumption Strategy.** A risk management strategy used to accept the risk.

**Risk Avoidance Strategy.** A risk management strategy used to avert the potential occurrence and/or consequence of a hazard by either selecting a different approach or not implementing a specific proposal.

**Risk control.** Risk control is a means to reduce or eliminate the effects of hazards.

**Risk Control Strategy.** A risk management strategy used to develop options and take actions to lower the risk.

**Risk Mitigation.** Refer to “Mitigation.”

**Risk Transfer Strategy.** A risk management strategy used to shift the ownership of a risk to another party.

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

**Safety Assurance.** Processes within the SMS that function systematically to measure safety performance and determine whether an organization meets or exceeds its safety objectives through the collection, analysis, and assessment of information.

**Safety Culture.** The way safety is perceived and valued in an organization. It represents the priority given to safety at all levels in the organization and reflects the real commitment to safety.

**Safety Directive.** A mandate from the CAA to take immediate corrective action to address a noncompliance issue that creates a significant unsafe condition.

**Safety Management System (SMS).** An integrated collection of processes, procedures, policies, and programs that are used to assess, define, and manage the safety risk in the provision of aviation-related services.

**Safety Margin.** The buffer between the actual minimum-level requirement and the limit of the hardware or software system.

**Safety objective**. Measurable goal or desirable outcome related to safety.

**Safety Performance**. Realized or actual safety accomplishment relative to the organization's safety objectives.

**Safety Performance Indicators (SPIs).** Metrics identified to determine how risk mitigations are performing. Also known as key performance indicators (KPIs). The SMS database prefers the interchangeable term KPI when referring to SPIs.

**Safety Performance Monitoring.** The act of observing the safety performance of the system to ensure an acceptable level of safety risk.

**Safety Performance Targets.** Measurable goals used to verify the predicted residual risk of a hazard. They should quantifiably define the predicted residual risk.

**Safety Policy.** The documented organizational policy that defines management’s commitment, responsibility, and accountability for safety. Safety Policy identifies and assigns responsibilities to key safety personnel.

**Safety Promotion.** The communication and distribution of information to improve the safety culture and support the integration and continuous improvement of the SMS within the company. Safety Promotion allows our company to share successes and lessons learned.

**Safety Requirement.** A planned or proposed means to reduce a hazard’s causes or effects.

**Safety Requirement Approval.** Certification that the safety requirements can and will be implemented.

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

**MOC SRM Document.** A documented safety analysis for a proposed Change or change stemming from an existing safety issue. It documents the evidence to support whether or not the proposed Change / existing safety issue is mitigated to an acceptable level from a safety risk perspective.

**MOC SRM Document Approval.** Indication that the MOC SRM document was developed properly; that hazards were systematically looked for and identified if applicable; and if a hazard was identified or safety risk was negatively impacted, that: 1) risk was appropriately assigned, 2) valid safety requirements were proposed, and an effective implementation and monitoring plan was prepared. MOC SRM document approval does not constitute acceptance of the risk associated with the Change or approval to implement the Change.

**SRM Committee.** A diverse group of representatives, stakeholders, and subject matter experts from the various departments affected by the Change. They conduct an objective safety analysis and provide findings and recommendations to decision-makers in an MOC SRM document.

**SRM Committee Facilitator.** A trained expert on the SRM process who moderates the deliberations of the SRM committee members from a neutral position. He or she captures the decisions of the committee members, mediates any disagreements, documents any dissenting opinions, and remains neutral throughout the process without advocating for a specific outcome. The facilitator/co-facilitator (or his or her designee) may write the safety document describing the safety findings of the SRM committee meeting.

**SRM Committee Member.** An SRM committee member is a stakeholder who represents the program, facility, organization, or constituency potentially affected by the safety risk and/or potential safety requirements associated with the Change and/or identified existing safety risk. The SRM committee members are selected at the discretion of the change proponent and/or committee facilitator.

**SRM Committee Observer.** An SRM committee observer is someone attempting to gain a better understanding of the SRM process, not the specific Change being assessed. An observer is not an active member of the SRM committee meeting and does not provide input during the deliberations. SRM committee observers are permitted at the discretion of the change proponent.

**SRM Practitioner.** Any person trained on SMS policy that uses any process to identify safety hazards, evaluate safety risk, and/or recommend activities that can affect safety of the provision of aviation-related services.

**Safety Risk Tracking.** A closed-loop means of ensuring that the requirements and mitigations associated with each hazard that has associated medium or high risk are implemented. Risk tracking is the process of defining safety requirements, verifying implementation, and reassessing the risk to make sure the hazard meets its risk level requirement before being accepted.

**Severity.** The consequence or impact of a hazard’s effect or outcome in terms of degree of loss or harm.

**Single Point Failure.** The failure of an item that would result in the failure of the system and is not compensated for by redundancy or an alternative operational procedure.

**SMS Continuous Improvement Plan.** The plan that specifies the activities required for individual departments to allocate sufficient resources toward the integration and maturation of the company SMS.

**Source (of a hazard).** Any real or potential origin of system failure, including equipment, operating environment, human factors, human-machine interface, procedures, and external services.

**Stakeholder.** A group or individual that is affected by or is in some way accountable for the outcome of a safety undertaking; an interested party having a right, share, or claim in a product or service, or in its success in possessing qualities that meet that party’s needs and/or expectations.

## 11.1 Acronyms

**ASAP.** The Aviation Safety Action Program (ASAP) is a voluntary reporting program in which airlines and other Part 121 operators team up with the FAA to enhance flight safety. The goal of ASAP is to detect problems and safety hazards in flight operations before those problems cause an accident.

**ASRS**. The Aviation Safety Reporting System captures confidential reports, analyzes the resulting data, and disseminates vital information to the aviation community.

**CPA**. Corrective Action and Preventive Action

**MOC**. Management of Change

**ORP**. Operational Risk Profile. Each area of operation within the company has unique hazards and associated risks. In SMS Pro, an ORP is a collection of hazards, risks and controls associated with a division’s operations.

**PHAT**. Proactive Hazard Analysis Tool