ADVISORY CIRCULAR

SUBJECT:	DATE:	AC NUMBER:	VERSION:
SAFETY MANAGEMENT SYSTEMS	2021-04-20	005-01	6.0

NOTE: THIS ADVISORY CIRCULAR IS PUBLISHED TO PROVIDE REGULATORY INFORMATION AND DESCRIBE ACCEPTABLE MEANS OF COMPLIANCE WITH THE GENERAL AUTHORITY OF CIVIL AVIATION REGULATIONS (GACAR).

CHAPTER 1 – BACKGROUND

1.1 Purpose.

The purpose of this Advisory Circular is to describe the framework of an acceptable Safety Management System (SMS) as well as acceptable means of compliance with the safety management system requirements of GACAR Part 5. Additionally, this Advisory Circular describes the processes for SMS implementation by aviation organizations (i.e., aviation service providers) and for the formal acceptance of the SMS by the General Authority of Civil Aviation (GACA). Lastly, this Advisory Circular describes an acceptable means of compliance with the phased implementation requirement for safety management systems as prescribed in GACAR Part 199.

1.2 Applicability.

This Advisory Circular is applicable to all aviation organizations required to have an SMS under the General Authority of Civil Aviation Regulations (GACAR) Part 5.

1.3 Cancellation.

This is the first official version of this Advisory Circular and it cancels no other Advisory Circulars.

1.4 Related Regulatory Provisions.

GACAR Parts 1, 5, 119, 121, 125, 135, 139, 141, 142, 145, 170, 171, 172, 173, 175, and 199.

1.5 Related Reading Material.

None.

1.6 Definitions of Terms Used in this Advisory Circular.

Affected parties should refer to Subpart A of GACAR Part 1 for a full listing of defined terms used in the new GACAR and specifically those related to safety management. This Advisory Circular introduces several additional definitions to aid in a common understanding of the ideas presented in this document. In cases where the definitions in this document differ from an identical term defined in GACAR Part 1, the definition in GACAR Part 1 will prevail when interpreting regulatory requirements.

1.7 Approval.

This Advisory Circular has been approved for publication by the Assistant President, Safety, Security and Air Transport (SS&AT) Sector of the General Authority of Civil Aviation.

CHAPTER 2 – THE SMS FRAMEWORK

2.1 Introduction.

The SMS framework is composed of components, elements, and processes, each of which is explained in terms of its functional expectations, or how they would need to be used in order to contribute to an effective SMS. These functional expectations are further defined in terms of performance objectives (what the process needs to do) and design expectations (what needs to be developed in order for the process to function as intended).

The SMS framework addresses two important needs:

a) To provide one standard set of concepts, documents, and tools for the development and implementation of SMS that complies with General Authority of Civil Aviation Regulation (GACAR) Part 5.

b) To make the SMS documents and tools align with the structure and format of the International Civil Aviation Organization (ICAO) SMS Framework.

The Framework describes the objectives and expectations for an aviation organization's SMS. The Framework is intended to address only operational and support processes and activities that are related to aviation safety and not to address those related to occupational safety, environmental protection, or customer service quality, all of which are outside of the scope of the GACAR.

Aviation organizations are responsible for the safety of services or products they purchase or contract from other organizations. This document describes the minimum objectives and expectations for an effective and compliant SMS; aviation organizations may establish additional or stricter requirements.

2.2 Scope.

This Framework provides guidance for SMS development by aviation organizations (e.g., air operators, repair stations, flight training organizations, air traffic service providers, and aerodrome operators) and forms the basis for SMS assessments which are described later in this document.

2.3 Applicability.

The President views the objectives and expectations in the Framework as a minimum for an aviation organization to develop and implement in order to comply with the SMS requirements as specified in GACAR Part 5.

2.4 References.

The Framework is in accordance with the following documents:

- ICAO Annex 19, Safety Management
- International Civil Aviation Organization (ICAO) Document 9859, 3rd Edition (as amended), ICAO Safety Management Manual (SMM)
- ICAO Document 9734, Safety Oversight Manual

2.5 Definitions.

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

b. Accountable Executive. The single, identifiable person having authority and final responsibility for the effective and efficient performance of the organization's SMS. Depending on the size and complexity of the organization, the Accountable Executive may be the chief executive officer (CEO), the chairperson of the board of directors, a partner, or the proprietor. The authorities and responsibilities carried out by the Accountable Executive include, but are not limited to:

a. full authority for human resources issues;

b. authority for major financial issues;

c. direct responsibility for the conduct of the organization's affairs;

d. final authority over operations under certificate; and

e. final responsibility for all safety issues.

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

d. Assessment. The process of measuring or judging the value or level of something.

e. Attributes. System Attributes, or the inherent characteristics of a system, are present in any well-defined organization and apply to an effective SMS. The six system safety attributes for the

purpose of this document are: Procedures; Controls; Process Measures; Interfaces; Responsibility; and Authority. Each safety attribute is defined in this section.

f. Audit. Scheduled, formal reviews and verifications that evaluate whether an organization has complied with policy, standards, and/or contract requirements. An audit starts with the management and operations of the organization and then moves to the organization's activities and products/services.

g. Authority. Who can direct, control, or change the process, as well as who can make key decisions such as risk acceptance. This attribute also includes the concept of empowerment.

h. Aviation System. The functional operation or production system used by an organization to produce an aviation product or service (see System and Functional below).

i. Complete. Nothing has been omitted and what is stated is essential and appropriate to the level of detail.

j. Conformity. Fulfilling or complying with a requirement [ref. ISO 9001-2000]; this includes but is not limited to complying with aviation safety regulations. It also includes complying with company requirements, requirements of operator-developed risk controls, or operator policies and procedures.

k. Continuous Monitoring. Uninterrupted (constant) watchfulness (checks, audits, etc.) over a system.

l. Controls. Controls are elements of the system, including hardware, software, special procedures or procedural steps, and supervisory practices designed to keep processes on track to achieve their intended results. Organizational process controls are typically defined in terms of special procedures, supervisory and management practices, and processes. Many controls are inherent features of the SMS Framework. Practices such as continuous monitoring, internal audits, internal evaluations, and management reviews (all parts of the safety assurance component) are identified as controls within the design expectations. Additionally, other practices such as documentation, process reviews, and data tracking are identified as controls within specific elements and processes.

m. Corrective Action. Action to eliminate (remove) or mitigate (lessen) the cause or reduce the effects of a detected nonconformity or other undesirable (unwanted) situation.

n. Correct. Accurate without ambiguity or error in its attributes.

o. Credible. Implies that it is reasonable to expect the assumed combination of extreme conditions will occur within the operational lifetime of the system.

p. Documentation. Information or meaningful data and its supporting medium (e.g., paper, electronic, etc.). In this context, documentation is different from records because documentation is the written description of policies, processes, procedures, objectives, requirements, authorities, responsibilities, or work instructions; whereas Records are the evidence of results achieved or activities performed.

q. Evaluation. An independent review of company policies, procedures, and systems. If accomplished by the company itself, the evaluation should be done by a person or organization in the company other than the one performing the function being evaluated. The evaluation process builds on the concepts of auditing and inspection. An evaluation is an anticipatory process designed to identify and correct potential problems before they happen. An evaluation is synonymous with the term "systems audit."

r. External Audit. An audit conducted by an entity outside of the organization being audited (e.g., the flight operations division audits the flight training department).

s. Functional. The term "function" refers to "what" is expected to be incorporated into each process (e.g., human tasks, software, hardware, procedures, etc.) rather than "how" the function is accomplished by the system. This makes for a more performance-based system and allows for a broad range of techniques to be used to accomplish the performance objectives. This, in turn, maximizes scalability while preserving standardization of results across the aviation organization communities.

t. Hazard. Any existing or potential condition or object that can lead to an accident, incident; or damage to the environment. A hazard is a condition that might cause (is a prerequisite to) an accident or incident.

u. Incident. It is a near-miss episode with minor consequences that could have resulted in greater loss, or an unplanned event that could have resulted in an accident or did result in minor damage. An incident indicates that a hazard or hazardous condition exists, though it may not identify what that hazard or hazardous condition is.

v. Interfaces. This aspect includes examining such things as lines of authority between departments, lines of communication between employees, consistency of procedures, and clearly delineating lines of responsibility between organizations, work units, and employees. Interfaces are the "Inputs" and "Outputs" of a process.

w. Interfaces in Safety Risk Management and Safety Assurance. Safety Risk Management (SRM) and Safety Assurance (SA) are the key processes of the SMS. They are also highly interactive, especially in the input-output relationships between the activities in the processes. This is especially important where interfaces between processes involve interactions between different

departments, contractors, etc. Assessments of these relationships should pay special attention to flow of authority, responsibility, and communication, as well as procedures and documentation.

x. Internal Audit. An audit conducted by, or on behalf of, the organization being audited (e.g., the flight training department audits the flight training department).

y. Lessons Learned. Knowledge or understanding gained by experience, which may be positive, such as a successful test or mission, or negative, such as a mishap or failure. Lessons learned should be developed from information obtained from inside and outside of the organization and/or industry.

z. Likelihood. The estimated probability or frequency, in quantitative or qualitative terms, of an occurrence related to the hazard.

aa. Line Management. The management structure that operates (controls, supervises, etc.) the operational activities and processes of the aviation system.

bb. Nonconformity. Non-fulfillment of a requirement [ref. ISO 9001-2000]. This could include but is not limited to, noncompliance with regulations, company requirements, requirements of operator-developed risk controls, or operator-specified policies and procedures.

cc. Objective. The desired state or performance target of a process. Usually it is the final state of a process and contains the results and outputs used to obtain the desired state or performance target.

dd. Operational Life Cycle. Period of time from implementation of a product/service until it is no longer in use.

ee. Organization. Indicates both certificated and non-certificated aviation organizations who are engaged in providing aviation services.

ff. Outputs. The product or end result of a SMS process that can be recorded, monitored, measured, and analyzed. Outputs are the minimum expectation for the product of each process area and the input for the next process area in succession. Each of the outputs of a process should have a method of measurement specified by the organization. Measures need not be quantitative where this is not practical; however, some method of providing objective evidence of the attainment of the expected output is necessary.

gg. Oversight. A function performed by a regulator (such as the GACA Safety and Air Transport Sector) that ensures that an aviation organization conforms with and uses safety-related standards, requirements, regulations, and associated procedures. A form of oversight can also result from a requirement to meet standards of a non-regulatory organization, e.g., the International Air Transport

Association (IATA).

hh. Preventive Action. Preemptive action to eliminate or mitigate the potential cause or reduce the future effects of an identified or anticipated nonconformity or other undesirable situation.

ii. Procedures. ISO-9001-2000 defines “procedure” as “a specified way to carry out an activity or a process.” Procedures translate the “what” in goals and objectives into “how” in practical activities (things people do). Procedures are simply documented activities to accomplish processes (e.g., a way to perform a process). The organization should specify their own procedures for accomplishing processes in the context of their unique operational environment, organizational structure, and management objectives.

jj. Process. A set of interrelated or interacting activities that transform inputs into outputs.

kk. Process Measures. Ways to provide feedback to responsible parties that required actions are taking place, required outputs are being produced, and expected outcomes are being achieved. A basic principle of safety assurance is that fundamental processes be measured so that management decisions can be data-driven. The general expectations for Component 1, Policy, specify that SMS outputs be measured and analyzed. These measurements and analyses are accomplished in Component 3, Safety Assurance. Outputs of each process should, therefore, be identified during Component 3 activities. For example, these outputs should be the subjects of continuous monitoring, internal audits, and internal evaluation.

ll. Product/Service. Anything that is offered or can be purchased that might satisfy a want or need in the air transportation system.

mm. Records. Evidence of results achieved or activities performed.

nn. Residual Safety Risk. The safety risk that exists after all controls have been implemented or exhausted and verified. Only verified/substantiated controls can be used for assessing residual safety risk.

oo. Responsibility. Who is accountable for management and overall quality of the process (planning, organizing, directing, controlling) and its ultimate accomplishment.

pp. Risk. The product of predicted severity (how bad) and likelihood (how probable) of the potential safety effect of a hazard in its worst credible (reasonable or believable) system state. The terms “risk” and “safety risk” are interchangeable.

qq. Risk Control. Steps taken to eliminate (remove) hazards or to mitigate (lessen) their effects by

reducing the severity and/or likelihood of risk associated with those hazards.

rr. Safety Assurance (SA). A formal management process within the SMS that systematically provides confidence that an organization's products/services meet or exceed safety requirements. A Safety Assurance flow diagram (found in section 5.4) includes the Framework element/process numbers and other notes to help the reader visualize the Framework in terms of a process flow (with interfaces), and understand the component/element/process expectations.

ss. Safety Culture. The product of individual and group values, attitudes, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, the organization's management of safety. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventive measures.

tt. Safety Management System (SMS). The formal, management driven business-like approach to managing safety risk. It includes systematic procedures, practices, and policies for the management of safety (as described in this document it includes safety risk management, safety policy, safety assurance, and safety promotion).

uu. Safety Planning. Part of safety management focused on setting safety objectives and specifying needed operational processes and related resources to fulfill these objectives.

vv. Safety Promotion. A combination of safety culture, training, communications and data-sharing activities that support the implementation and operation of an SMS in an organization.

ww. Safety Risk. The product of predicted severity (how bad) and likelihood (how probable) of the potential safety effect of a hazard in its worst credible (reasonable or believable) system state. The terms "safety risk" and "risk" are interchangeable.

xx. Safety Risk Control. A characteristic of a system that reduces or mitigates (lessens) the potential undesirable effects of a hazard. Controls may include process design, equipment modification, work procedures, training, or protective devices. Safety risk controls must be written in requirements language, measurable, and monitored to ensure effectiveness.

yy. Safety Risk Management (SRM). A formal process within the SMS that describes the system, identifies the hazards, analyses the risk, assesses the risk, and controls the risk. The SRM process is embedded in the processes used to provide the product/service; it is not a separate/distinct process.

zz. Separate Aviation Maintenance Organizations. Independent maintenance organizations such as, but not limited to, certificated repair stations, non-certificated repair facilities, and separate

maintenance organizations. This does not include an air operator's integral maintenance organization.

aaa. Severity. The degree of loss or harm resulting from a hazard.

bbb. Substitute Risk. A risk unintentionally created as a consequence of safety risk control(s).

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

ddd. System Attributes. Refer to definition for Attributes, above.

eee. Top Management. The person or group of people who direct and control an organization. In many large organizations, this can be the board of directors; in smaller organizations, this might be the owner of the company. The accountable executive generally heads the top management.

fff. Worst. The most unfavorable conditions expected.

CHAPTER 3 - SMS FRAMEWORK STRUCTURE AND EXPECTATIONS

3.1 SMS Framework Structure.

The SMS Framework is broken down into components, elements, and processes. The components and elements are based on the ICAO SMS Framework.

3.2 Components.

There are four components of an SMS. Two components represent the core operational activities underlying an SMS, and two components represent the organizational arrangements that are necessary to support the two core operational activities. The four components of an SMS are:

(1) Safety Policy and Objectives (Component 1.0)

(2) Safety Risk Management (SRM) (Component 2.0)

(3) Safety Assurance (SA) (Component 3.0)

(4) Safety Promotion (Component 4.0)

The two core operational activities of an SMS are Safety Risk Management and Safety Assurance. Further detailed guidance on the processes and tools that are commonly associated with Safety Risk Management activities are located in Appendix D of this Advisory Circular.

3.3 Elements.

Each of the four components of an SMS is further subdivided into elements, each of which defines important aspects of the component. There are twelve elements in the SMS framework arranged as follows:

For Component 1.0 - Safety Policy and Objectives

(a) Element 1.1 - Safety policy

(b) Element 1.2 - Management commitment and safety accountabilities

(c) Element 1.3 - Key safety personnel

(d) Element 1.4 - Emergency preparedness and response

(e) Element 1.5 - SMS documentation and records

For Component 2.0 - Safety Risk Management (SRM)

(a) Element 2.1 - Hazard identification and analysis

(b) Element 2.2 - Risk assessment and control

For Component 3.0 - Safety Assurance (SA)

(c) Element 3.1 - Safety performance monitoring and measurement

(d) Element 3.2 - The management of change

(e) Element 3.3 - Continuous improvement

For Component 4.0 - Safety Promotion

(f) Element 4.1 - Competencies and training.

(g) Element 4.2 - Communication and awareness.

3.4 Processes.

Certain elements in the Safety Risk Management, Safety Assurance and Safety Promotion components are further broken down into processes.

3.5 SMS Framework Expectations.

To make the SMS Framework easier to understand and use, components, elements, and processes have been defined in terms of functional expectations, or how an organization would need to use them in order for them to contribute to an effective SMS. They are called “functional” expectations because they describe the “what”, not the “how” of each process. For example, the “what” of a de-icing process is to prevent any aircraft from taking off with ice adhering to any critical control surface. The “how” of the de-icing process would include de-icing equipment procedures, flight crew de-icing procedures, holdover table activities, etc., and may be different between individual organizations. Organizations are expected to meet SMS Framework expectations by developing processes to fit their unique business and management models.

The SMS functional expectations are further defined in terms of performance objectives and design

expectations:

(1) Performance Objectives. Performance Objectives are the desired outcomes of the particular element or process.

(2) Design Expectations. Design Expectations are the characteristics of the element or process that, if properly implemented, should provide the outcomes identified in the performance objectives.

The Performance Objectives and Design Expectations for the entire SMS Framework is found in Appendix A of this Advisory Circular.

CHAPTER 4 - SMS IMPLEMENTATION

4.1 Purpose.

This chapter contains guidance, expectations, and procedures necessary to implement a SMS by aviation organizations that are eligible for a phased implementation of a SMS, as provided for by the GACAR Part 199.

4.2 Applicability.

The implementation guidance is designed for use in designing and managing an existing aviation organization's SMS phased implementation activities. Phased implementation guidance is not designed to be used by new applicants wishing to commence operations under GACAR Parts 121, 125, 135, 139, 141, 142, 145 or 171. These aviation organizations are required to have an SMS implemented at the time of their initial certification.

4.3 References.

The following references are recommended reading material for users of this implementation guidance in development and implementation of an SMS:

- International Civil Aviation Organization (ICAO) Document 9859, 3rd Edition, ICAO Safety Management Manual (SMM)
- SMS Framework Description in this document
- SMS Assessment Description in this document

4.4 Guidance and Tools.

The GACA developed SMS Framework guidance is the standard for implementation of SMS by aviation organizations. It is similar in scope and format to International Organization for Standardization (ISO) standards and is modeled after the safety, quality, and environmental management standards developed by a variety of organizations such as ISO, the British Standards Institute, Transport Canada, Standards Australia, and the International Air Transportation Association (IATA). The SMS Framework also incorporates the current requirements of ICAO, and it is closely aligned with the current ICAO SMS Framework.

a) *SMS Assessment Guidance.* The GACA has developed SMS Assessment Guidance as a tool, included in this document as Appendix C, for aviation organizations and GACA SS&AT staff.

The SMS Assessment Guidance represents each functional expectation found in the SMS Framework in the form of a question and is intended to be used during the development and implementation of a SMS by an organization or by the GACA SS&AT staff for oversight guidance. Since the SMS Assessment Guidance is based entirely on the SMS Framework, compliance with the SMS Assessment Guidance will ensure compliance with the SMS Framework.

b) *SMS Implementation Guidance.* The SMS Implementation Guidance contains the expectations and procedures necessary to implement an SMS.

c) *Gap Analysis Processes and Tools*. An initial step in developing an SMS is for the aviation organization to analyze and assess its existing programs, systems, processes, and activities with respect to the SMS functional expectations found in the SMS Framework. This process is called a "gap analysis"; the "gaps" being those elements in the SMS Framework that are not already being performed by the aviation organization.

NOTE: The gap analysis processes cover all areas of company operations that are subject to regulatory control in accordance with the GACARs and all elements of the SMS Framework.

4.5 Roles, Responsibilities and Relationships.

The SMS Framework provides guidance for an aviation organization to develop and document its SMS. A separate SMS manual is not specifically required; however, many organizations find a separate manual useful. The SMS may be documented in a form and manner that best serves the organization's need; however, any modifications of existing GACA SS&AT approved/accepted programs and their associated documents must be coordinated with the GACA SS&AT. Safety policies developed by organizations' top management will be clearly communicated throughout the entire organization. Safety Risk Management (SRM) and Safety Assurance (SA) programs will be developed and maintained. Safety Promotion (SP) activities will take place to instill or reinforce a positive safety culture throughout the organization.

The GACA SS&AT office that normally provides regulatory safety oversight of the aviation organization will be referred to as the "oversight organization" and will continue all of its normal oversight and certificate management duties. As organizations develop their SMS, a natural interaction between the safety management efforts of the oversight organization and those of the aviation organization will develop. This relationship can leverage the efforts of both parties to provide a more effective, efficient, and proactive approach to meeting safety requirements while at the same time increasing the flexibility of the aviation organization to tailor their safety management efforts to their individual business models.

• The aviation organization should expect the oversight organization to be fully engaged during SMS development and implementation.

• Specifically, the oversight organization will:

• Oversee and review gap analysis processes

• Review and accept the aviation organization's implementation plan and other documents

• Discuss the requirements of the exit criteria for all implementation phases with the aviation organization. Exit criteria are those SMS development activities that must be completed prior to moving to the next implementation phase

4.6 SMS Implementation Strategy.

a) *Phased Implementation.* Initial SMS implementation strategy follows a four-phased process similar to that outlined in the ICAO Safety Management Manual (SMM). ICAO, as well as many other States that are in the process of implementing SMS requirements, favors a phased implementation process. The SMS implementation guidance presented in this document closely parallels the ICAO recommended phased implementation process outlined in ICAO Document 9859. The phases of implementation are arranged in four levels of implementation "maturity". The timeline and milestone requirements for each implementation phase are according to the requirements outlined in the GACAR Part 199. The four phases (and implementation levels) of phased SMS implementation are:

Level 1 (ICAO Phase I) — Planning & Organizing SMS implementation;

Level 2 (ICAO Phase II) — Reactive Processes, Basic Safety Risk Management;

Level 3 (ICAP Phase III) — Proactive Processes, Looking Ahead; and

Level 4 (ICAO Phase IV) — Continuous Improvement, Continued Assurance.

Note: A summary diagram of the different phases of implementation can be found in the ICAO Safety Management Manual, Chapter 10.

b) *The development and implementation of an SMS.* This task is best accomplished by breaking down the task into smaller, more manageable subcomponents. In this way, overwhelming and sometimes confusing complexity, and its underlying workload, may be turned into simpler and more transparent subsets of activities that only require minor increases in workloads and

resources. This partial allocation of resources may be more commensurate with the requirements of each activity as well as the resources available to the aviation organization.

c) *Justification.* The reasons that justify why a phased approach to SMS implementation is recommended can be expressed as: (a) providing a manageable series of steps to follow in implementing an SMS, including allocation of resources; and (b) effectively managing the workload associated with SMS implementation.

d) *Cosmetic Compliance.* An aviation organization should set as its objective the realistic implementation of a comprehensive and effective SMS, not the tokens of it. You simply cannot "buy" an SMS system or manual and expect the benefits of a fully implemented SMS.

e) *Feedback.* Implementation experiences have shown that while full SMS implementation will certainly take longer, the robustness of the resulting SMS will be enhanced and early benefits realized as each implementation phase is completed. In this way, simpler safety management processes are established and benefits realized before moving on to processes of greater complexity. This is especially true with regard to Safety Risk Management (SRM). In the reactive phase (Level 2), an aviation organization will build an SRM system around known hazards that are already identified. This allows company resources to be focused on developing risk analysis, assessment and control processes (that frequently resolve old long-term issues and hazards) unencumbered by the complexities necessary at the proactive (Level 3) and predictive phases (Level 4).

f) *Summary.* Guidance for a phased implementation of SMS aims at:

- Providing a manageable series of steps to follow in implementing an SMS, including allocation of resources,
- Effectively managing the workload associated with SMS implementation
- Pre-empting a "box checking" exercise
- Realization of safety management benefits and return on investment during an SMS implementation project

4.7 Implementation Levels.

The overall objective of the levels is to develop and implement an integrated, comprehensive SMS for the organization.

Implementation Orientation & Commitment. SMS implementation by the aviation organization begins with a recognition by the aviation organization that the GACAR Part 5 is applicable, and the aviation organization's top management commitment to begin the steps of initiating the SMS development process, including gathering necessary information, evaluating corporate goals and objectives, and committing resources to the SMS implementation effort.

Implementation Level One: Planning and Organization. Level One begins when an aviation organization's top management commits to providing the resources necessary for full implementation of SMS throughout the organization.

i *Gap Analysis*. The first step in developing an SMS is for the aviation organization to analyze its existing programs, systems, and activities with respect to the SMS functional expectations found in the SMS Framework. This analysis is a process and is called a "gap analysis," the "gaps" being those components, elements and processes in the SMS Framework that are not already being performed by the aviation organization.

- The Gap Analysis process should consider and encompass the entire organization (e.g., functions, processes, organizational departments, etc.) to be covered by the SMS.

- The gap analysis should be continuously updated as the aviation organization progresses through the SMS implementation process

ii *Implementation Plan*. Once the gap analysis has been performed, an implementation plan is prepared. The implementation plan is simply a "road map" describing how the aviation organization intends to close the existing gaps by meeting the objectives and expectations in the SMS Framework. The implementation plan must be accepted by the GACA before specific implementation activities incorporated in the plan can be considered finalized.

- While no actual development activities are expected during level one, beyond those listed in the SMS Framework, Elements 1.1, 1.2 (partial), 1.3 and 4.1.1 (partial), the aviation organization organizes resources, assigns responsibilities, sets schedules, and defines objectives necessary to address all gaps identified.

- It should be noted that at each level of implementation, top management's approval of the implementation plan must include allocation of necessary resources IAW Element 1.2.

iii *Level 1 – Exit Expectations.* The following items are required prior to Level 1 exit:

- Objective evidence of top management's commitment to implement SMS, define safety

policy and convey safety expectations and objectives to all employees

• Objective evidence of top management's commitment to insure adequate resources are available to implement SMS

• Designation of an accountable executive who will be responsible for SMS development

• Definition of safety-related positions for those who will participate in SMS development and implementation

• Completed gap analysis on the entire organization for all elements of the SMS Framework

• Completed comprehensive SMS implementation plan for all elements to take the organization through Level 4. This SMS implementation plan must be accepted by GACA.

• Identified safety competencies required, completed training appropriate to Level 1, implementation phase identified for competencies required, and a training plan for all employees

Implementation Level Two: Reactive Process, Basic Safety Risk Management. At level two, the aviation organization develops and implements a basic SRM process and plan, and organizes and prepares the organization for further SMS development. Information acquisition, processing, and analysis functions are implemented and a tracking system for risk control and corrective actions are established. At this phase, the aviation organization corrects known deficiencies in safety management practices and operational processes, develops an awareness of hazards, and responds with appropriate systematic application of preventative or corrective actions. This allows the aviation organization to react to unwanted events and problems as they occur and develop appropriate remedial action. For this reason, this level is termed "reactive."

i *Level 2 – Exit Expectations.* The following items are required prior to Level 2 exit:

• Processes and procedures documented for operating the SMS to the level of reactive analysis, assessment and mitigating actions

• Develop documentation relevant to SMS implementation plan and SRM components (reactive processes)

• Document and initiate voluntary non-punitive employee reporting and feedback program;

• Completed SMS training for the staff directly involved in the SMS process and initiated training for all employees to at least the level necessary for the SMS reactive processes

• Apply Safety Risk Management (SRM) processes and procedures to at least one known (existing) hazard and initiate the mitigation process to control/mitigate the risk associated with the hazard

• Update the detailed gap analysis on the entire organization for all elements of the SMS Framework

• Update the comprehensive SMS implementation plan for all elements to take the organization through Level 4

Implementation Level Three: Proactive Processes, Looking Ahead. The activities involved in the SRM processes involve careful analysis of systems and tasks involved; identification of potential hazards in these functions; and development of risk controls. The risk management process developed at level two is used to analyze, document, and track these activities. Because the aviation organization is now using the processes to look ahead, this level is termed “proactive.” At this level, however, these proactive processes have been implemented but their performance has not yet been proven. (Fully functioning SMS) Component 2.0 of the SMS Framework expects SRM to be applied to:

• Initial design of systems, processes, organizations, and products

• Development of operational procedures

• Planned changes to operational processes

i *Level 3 – Exit Expectations.* The following items are required prior to Level 3 exit:

• Demonstrated performance of Level 2 requirements

• Objective evidence that all SMS processes are being updated, maintained and practiced

• Objective evidence that the Safety Risk Management process has been

conducted on all Component 2.0 operating processes

• Objective evidence of compliance with Process 2.1.1

• Objective evidence of compliance with Element 3.2

• Objective evidence of compliance with Element 4.1

• Objective evidence of compliance with Process 4.1.1

• All applicable SMS processes and procedures must have been applied to at least one existing hazard and the mitigation process must have been initiated

• Complete SMS training for the staff directly involved in the SMS process to the level of accomplishing all SMS processes

• Complete employee training commensurate with the requirements of Level 3

Implementation Level Four: Continuous Improvement, Continued Assurance. The final level of SMS maturity is the continuous improvement level. Processes have been in place, and their performance and effectiveness have been verified. The complete SA process, including continuous monitoring and the remaining features of the other SRM and SA processes are functioning. A major objective of a successful SMS is to attain and maintain this continuous improvement status for the life of the organization.

4.8 Analysis Processes.

Guidance and tools have been developed for use in directing and evaluating progress though the SMS implementation process. These tools are based on performance objectives and design expectations developed for each Component, Element, and Process of the SMS Framework.

• The SMS Framework is based on ICAO and GACA requirements/guidance

• The SMS Assessment Guide is based upon the SMS Framework, in question form

• The Gap Analysis Tools are based upon the ICAO SMS Gap Analysis tools in a user-friendly format

System Description and Analysis. Prior to performing the gap analysis process, the aviation organization should conduct an analysis of all of the organization's operational functions,

programs, processes, and documentation in order to fully understand how their existing operations compare to the SMS framework.

Gap Analysis. The phased implementation of an SMS requires an aviation organization to conduct an analysis of its system to determine which components and elements of an SMS are currently in place and which components and elements must be added or modified to meet the implementation requirements. This analysis is known as gap analysis, and it involves comparing the SMS requirements against the existing resources of the aviation organization. A gap analysis tool based on the ICAO SMS Gap Analysis tool (Ref. ICAO SMM) can be used by aviation organizations. The GACA Assessment Tool that can be used as a gap analysis tool is in Appendix C of this document. The gap analysis tool provides, in checklist format, information to assist in the evaluation of the components and elements that comprise the SMS framework and to identify the components and elements that will need to be developed. Each question in the checklist is designed for a "Yes" or "No" response. A "Yes" answer indicates that the aviation organization already has the component or element of the SMS framework in question incorporated into its system and that it either matches or exceeds the requirement. A "No" answer indicates that a gap exists between the component/element of the SMS framework and the aviation organization's system. Once the gap analysis is complete and documented, it will form one basis of the SMS implementation plan.

4.9 Implementation Plan.

Based on the results of the gap analysis process, an implementation plan is prepared to "fill the gaps", the "gaps" being those elements in the SMS Framework that have not completely met expectations (e.g., are not already being performed) by the aviation organization. The SMS implementation plan is a realistic strategy for the implementation of an SMS that will meet the aviation organization's safety objectives while supporting effective and efficient delivery of services. It describes how the aviation organization will achieve its corporate safety objectives and how it will meet any new or revised safety requirements, regulatory or otherwise. Further guidance on how to develop an SMS implementation plan is contained in the ICAO SMM.

The implementation plan need not be complex or excessively detailed, but should provide a basic roadmap to meet the overall objective stated in the SMS Framework to, "…develop and implement an integrated, comprehensive SMS for [the] entire organization."

The implementation plan may consist of more than one document, details the actions to be taken, by whom and within what time-frame. The implementation plan can be created in any format that is useful to the company but should provide at least the following:

• Component/element/process reference from the SMS Assurance guidance or SMS Framework,

• Brief description of the actions to be taken and manual(s) affected,

• Responsible organization and/or individual(s), and

• Expected completion date.

The Implementation Plan should span the entire SMS development process. Consideration of it should be a part of the discussions from the earliest stages of SMS planning and organization, and appropriate adjustment of it should continue through all levels of SMS implementation maturity. It should be updated as necessary (along with the detailed gap analysis) as the projects progress. At each level, top management's approval of the implementation plan must include allocation of necessary resources IAW element 1.2.

CHAPTER 5 - SMS ACCEPTANCE

5.1 Introduction.

The objective of this chapter is to provide general information about GACA inspector responsibilities and activities for accepting or rejecting an aviation organization's Safety Management System (SMS). The SMS acceptance information addresses two important scenarios for an aviation organization's SMS proposal:

1. To accept or reject the development and implementation of a SMS, that complies with GACAR Part 5, for a new aviation organization seeking initial certification.

2. To accept or reject the development and implementation of a SMS, that complies with GACAR Part 5, for a currently certificated aviation organization eligible for the phased implementation process provided by the regulation.

This information is about the acceptance of a proposed SMS developed by aviation organizations (for example, air operators, flight training schools and training centers, and aerodrome operators) requiring certification by the GACARs.

5.2 References.

This information is in accordance with the following documents:

- ICAO Annex 19, Safety Management
- International Civil Aviation Organization (ICAO) Document 9859, 3rd Edition, ICAO Safety Management Manual (SMM)
- ICAO Document 9734, Safety Oversight Manual

5.3 New Aviation Organization Certification – SMS Acceptance.

It will be a responsibility of the GACA Aviation Safety Inspector (Inspector) to make an assessment of a proposed Safety Management System (SMS) submitted by a prospective aviation organization as part of the overall certification process. The assessment and acceptance of the proposed SMS will be by determination that the proposal is in accordance with the SMS framework described in this document. The assessment activities related to the acceptance of an SMS will be focused primarily on whether the applicant has implemented an SMS that meets all of the design expectations (i.e. design assessments) defined in the SMS framework. The assessment of the actual performance of the SMS (i.e.

performance assessments) will occur after the initial SMS acceptance.

Requirements. The objectives and expectations outlined in the framework represent the minimum standard for an aviation organization to develop and implement in order to comply with the SMS requirements as specified in GACAR Part 5. The framework describes the objectives and expectations for an aviation organization's SMS. The framework is intended to address only operational and support processes and activities that are related to aviation safety and not to address those related to occupational safety, environmental protection, or customer service quality. In addition, aviation organizations are responsible for the safety of services or products they purchase or contract from other organizations. The framework establishes the minimum objectives and expectations for an effective and compliant SMS; aviation organizations may establish additional or stricter requirements.

Assessment Tools and Techniques. As the Inspectors work through the process of assessing the proposed SMS for a new aviation organization's certification, there are two primary determinations that will be made to find the proposal acceptable: first, that the proposed SMS includes all the items required by the SMS framework; and, second, that the design expectations required by the framework have been adequately met by the documentation in the proposed SMS. The primary tool for assessing and accepting the proposed SMS is the acceptance tool found in Appendix B of this document and the assessment tool that is found in Appendix C of this document. The SMS Assessment Guide was developed to aid in the assessment of the design of aviation organizations' SMS programs in order to ensure that they comply with the SMS requirements specified in GACAR Part 5. For each required component, element and process, the SMS Assessment Guide includes:

- A brief statement of the performance objective
- A series of questions that are used to assess (i.e. evaluate) whether the design expectations have been met
- A "bottom line assessment" question is also included but this is only used during the periodic performance assessments.

Assessors, whether performing an assessment for the aviation organization or the GACA, should ask each question that pertains to the component, element or process under review and document their observations. From these assessments, the determination is made whether the SMS is meeting the minimum standards as specified in GACAR Part 5.

Agreement on the Aviation Organization's Safety Performance Indicators and Targets. In accordance with applicable GACA inspector guidance, the Inspector will ensure that agreement is reached and documented with the aviation organization as to the safety performance indicators,

values and targets (goals) as part of the acceptance process and prior to formal SMS acceptance. This concept is described in more detail later in this document.

Formal SMS Acceptance. For new certification programs (i.e. new aerodrome, new repair station, new air operators, etc.) the formal acceptance of the SMS occurs at the time of certificate issuance. In accordance with the requirements of GACAR Part 5, the SMS is considered formally accepted when the President of the GACA, or his representative designated for the purpose of SMS acceptance, has specifically endorsed the aviation organization certification documentation for SMS acceptance, Formal SMS acceptance will be communicated to the aviation organization in writing.

5.4 Currently Certificated Aviation Organizations - SMS Acceptance.

It will be a responsibility of the GACA Aviation Safety Inspector (Inspector) to accept or reject implementation plans and implementation levels (phases) of a proposed SMS submitted by aviation organizations (air operators, repair stations, flight training organizations aerodromes, etc.) that are eligible for a phased implementation of a SMS, as provided for by the GACAR. The acceptance process will focus on determining that the requirements for phased implementation outlined in Section 5 of this document, including the completion of all the steps in the implementation plan, are met.

CHAPTER 6 - AGREEMENT ON THE AVIATION ORGANIZATION'S SAFETY PERFORMANCE OBJECTIVES

Fundamental to safety management is the concept of continuous improvement and in order to achieve this it is necessary to have an ongoing knowledge of the level of safety within the system of the aviation organization. Determining the level of safety achieved, and comparing this to the minimum acceptable level of safety established by the aviation organization's safety policy and objectives, depends upon identifying, measuring and tracking safety indicators relative to safety targets established.

As part of the GACA Inspectors' oversight responsibilities, inspectors will establish agreements with aviation organizations about their safety performance indicators, safety performance indicator values to be used, safety performance target values as goals, and a plan to track indicator values and actions taken to achieve their target goals. This activity is associated with Element 1.1 of the aviation organization's SMS.

In order to structure an agreement with a particular aviation organization on safety performance indicators, values and targets to be used by the aviation organization, the individual operational environment for that aviation organization will be carefully considered.

The safety performance of the aviation organization related to the agreed upon safety indicators, values and goals must be tracked on a continual basis by the aviation organization in accordance with Component 3.0 (most notably Element 3.1) of the SMS Framework. This tracking activity and the readjustment of safety performance indicators and targets by the aviation organization, with the GACA agreement, will be reviewed periodically by the GACA as a part of Inspector oversight surveillance activities.

CHAPTER 7 - CONCLUSIONS

The implementation of SMS represents a fundamental shift in the way we all do business. A SMS requires aviation organizations to adopt the components and elements detailed in this document and to incorporate them into their everyday business practices. SMS is also being integrated into the international arena with the introduction of International Civil Aviation Organization (ICAO) SMS requirements for all ICAO Contracting States.

Fundamental to the SMS is the development of a robust regulatory framework that accommodates safety management systems. GACAR Part 5 has been developed to meet the regulatory need.

The GACA has structured the system of oversight to accommodate the SMS framework and operational requirements of the aviation organizations. In the future, the GACA will oversee the effectiveness of the SMS. Interventions will focus on the systems in place to manage the organization‘s operations and the outputs of the system, rather than focusing oversight activities on line-by-line adherence to the regulations through rigorous inspections and auditing.

The aviation organization must have effective programs in place to identify, analyze and correct safety issues, with minimal intervention at the operational level from the GACA. This approach does not constitute self-regulation nor does it represent an abrogation of the role of the regulator for the oversight of the aviation organization. Aviation organizations will be required to involve the GACA when issues are identified through their SMS. This will provide the GACA with an awareness that the aviation organization‘s SMS is working effectively. The success of the system depends on the development of a safety culture that promotes open reporting, through the adoption of safety reporting policies and continual improvement through, proactive safety assessments and quality assurance. The SMS philosophy requires that responsibility and accountability for safety be retained within the management structure of the organization. The accountable executive and top management are ultimately responsible for safety, as they are for other aspects of the aviation organization. However, every member of the aviation organization has safety responsibilities, as well; in safety management, everyone has a role to play.

- END -

COMPONENT 1.0 – SAFETY POLICY AND OBJECTIVES

Component Performance Objectives

The organization will develop and implement an integrated, comprehensive SMS for its organization and will incorporate a procedure to identify and maintain compliance with all applicable regulatory requirements.

Component General Design Expectations:

A. Safety management will be included in the complete scope and life cycle of the organization's systems including:

1) For air operators:

- Flight operations
- Operational control (dispatch/flight following)
- Maintenance and inspection
- Cabin safety
- Ground handling and servicing
- Cargo handling
- Training

2) For separate aviation maintenance organizations:

- Parts/materials
- Resource management (tools and equipment, personnel, and facilities)
- Technical data
- Maintenance and inspection
- Quality control

- Records management
- Contract maintenance
- Training

3) For pilot training organizations:

- Resource management (equipment, personnel, and facilities)
- Technical data
- Records management
- Contract maintenance
- Training program design and maintenance

4) For aerodromes:

- Runways
- Taxiways
- Run-up areas
- Ramps
- Apron areas
- On-airport fuel farms
- Operations and Maintenance
- Wildlife management
- Fire and Rescue
- Training

5) For air traffic services providers:

- Air traffic control operations and procedures
- Air traffic control facilities
- Air navigation facilities
- Air navigation facilities maintenance operations
- Air navigation procedures development and implementation
- Training

B. SMS processes will be:

- Documented
- Monitored
- Measured
- Analyzed

C. SMS outputs will be:

- Recorded
- Monitored
- Measured
- Analyzed

D. It is expected that:

- The organization will promote the growth of a positive safety culture (described under Component 4.0, B)
- If the organization has a quality policy, top management will ensure that the quality policy is consistent with the SMS
- The SMS will include a means to comply with all applicable GACA regulatory requirements.

• The organization will establish and maintain a procedure to identify all applicable current and forthcoming GACA regulatory requirements applicable to the organization

• The organization will establish and maintain procedures with measurable criteria to accomplish the objectives of the safety policy

• The organization will establish and maintain supervisory and operational controls to ensure procedures are followed for safety-related operations and activities

• The organization will establish and maintain a safety management plan to describe how it will achieve its safety objectives

Element 1.1 - Safety Policy

Performance Objective:

Top management will define the organization's safety policy and convey its expectations and objectives to its employees.

Design Expectations:

A. Top management will define the organization's safety policy.

B. The safety policy will:

- Include a commitment to implement an SMS
- Include a commitment to continual improvement in the level of safety
- Include a commitment to the management of safety risk
- Include a commitment to comply with applicable regulatory requirements
- Include a commitment to encourage employees to report safety issues without reprisal (as per Process 3.1.6)
- Establish clear standards for acceptable behavior
- Provide management guidance for setting safety objectives
- Provide management guidance for reviewing safety objectives
- Be documented
- Be communicated with visible management endorsement to all employees and responsible parties
- Be reviewed periodically to ensure it remains relevant and appropriate to the organization
- Identify responsibility and accountability of management and employees with respect to safety performance

Element 1.2 - Management Commitment and Safety Accountabilities

Performance Objective:

The organization will define, document, and communicate the safety roles, responsibilities, and authorities throughout its organization.

Design Expectations:

A. Top management will have the ultimate responsibility for the SMS.

B. Top management will provide resources essential to implement and maintain the SMS.

C. Aviation safety-related positions, responsibilities, and authorities will be:

- Defined
- Documented
- Communicated throughout the organization

D. The organization will define levels of management that can make safety risk acceptance decisions.

Element 1.3 - Key Safety Personnel

Performance Objective:

The organization will appoint a safety manager to manage, monitor, and coordinate the SMS processes.

Design Expectations:

A. Top management will appoint a member of management who, irrespective of other responsibilities, will have responsibilities and authority that includes:

- Ensuring that processes needed for the SMS are established, implemented, and maintained
- Report to top management on the performance of the SMS and the need for improvement
- Ensure the promotion of awareness of safety expectations throughout the organization

Element 1.4 - Emergency Preparedness and Response

Performance Objective:

The organization will develop and implement procedures that it will follow in the event of an accident or incident to mitigate the effects of these events.

Design Expectations:

A. The organization will establish procedures to:

- Identify hazards that have potential for accidents and incidents
- Coordinate and plan the organization’s response to accidents and incidents
- Execute periodic exercises of the organization’s response

Element 1.5 - SMS Documentation and Records

Performance Objective:

The organization will have documented safety policies; objectives, procedures, a document/record management process, and a safety management plan that meet organizational safety expectations and objectives.

Design Expectations:

A. The organization will establish and maintain information, in paper or electronic form, to describe:

- Safety policies
- Safety objectives
- SMS expectations
- Safety procedures and processes
- Responsibilities and authorities for safety-related procedures and processes
- Interactions/interfaces between the safety-related procedures and processes
- SMS outputs

B. The organization will maintain their safety management plan in accordance with the objectives and expectations contained within this element (1.5).

C. Documentation Management.

1) Documentation will be:

- Legible
- Dated (with dates of revisions)
- Readily identifiable
- Maintained in an orderly manner

• Retained for a specified period of time as determined by the organization

2) The organization will establish and maintain procedures for controlling all documents required by this Framework to ensure that:

• They can be located

• They are periodically:

o Reviewed

o Revised as needed

o Approved for adequacy by authorized personnel

3) The current versions of relevant documents are available at all locations where essential SMS operations are performed.

4) Obsolete documents are promptly removed from all points of use or otherwise assured against unintended use.

D. Records Management.

1) The organization will establish and maintain procedures to:

• Identify

• Maintain

• Dispose of their SMS records

2) SMS records will be:

• Legible

• Identifiable

• Traceable to the activity involved

3) SMS records will be maintained in such a way that they are:

- Readily retrievable
- Protected against:
    - o Damage
    - o Deterioration
    - o Loss

4) Records retention times will be documented.

COMPONENT 2.0 – SAFETY RISK MANAGEMENT (SRM)

Component Performance Objective:

The organization will develop processes to understand the critical characteristics of its systems and operational environment and apply this knowledge to identify hazards, analyze and assess risk, and design risk controls.

Component General Design Expectations:

A. Safety Risk Management (SRM) will, at a minimum, include the following processes:

- System and task analysis
- Hazard identification
- Safety risk analysis
- Safety risk assessment
- Safety risk control and mitigation

B. The SRM process will be applied to:

- Initial designs of systems, organizations, and/or products
- The development of operational procedures
- Hazards that are identified in the safety assurance functions (described in Component 3.0, B)
- Planned changes to operational processes

C. The organization will establish feedback loops between assurance functions described in Component 3.0 to evaluate the effectiveness of safety risk controls.

D. The organization will define a risk acceptance process that:

- Defines acceptable and unacceptable levels of safety risk.
- Describes:

o Severity levels

o Likelihood levels

• Defines specific levels of management that can make safety risk acceptance decisions

• Defines acceptable risk for hazards that will exist in the short-term while safety risk control/mitigation plans are developed and executed

Element 2.1 - Hazard Identification and Analysis

Process 2.1.1 - System Description and Task Analysis

Performance Objective:

The organization will analyze its systems, operations, and operational environment to gain an understanding of critical design and performance factors, processes, and activities to identify hazards.

Design Expectations:

A. System descriptions and task analysis will be developed to the level of detail necessary to:

- Identify hazards
- Develop operational procedures
- Develop and implement risk controls

Element 2.1 - Hazard Identification and Analysis

Process 2.1.2 - Identify Hazards

Performance Objective:

The organization will identify and document the hazards in its operations that are likely to cause death, serious physical harm, or damage to equipment or property in sufficient detail to determine associated level of risk and risk acceptability.

Design Expectations:

A. Hazards will be:

- Identified for the entire scope of the system, as defined in the system description
- Documented

B. Hazard information will be:

- Tracked
- Managed through the entire SRM process

Element 2.2 - Risk Assessment and Control

Process 2.2.1 - Analyze Safety Risk

Performance Objective:

The organization will determine and analyze the severity and likelihood of potential events associated with identified hazards, and will identify factors associated with unacceptable levels of severity or likelihood.

Design Expectations:

A. The safety risk analysis process will include:

- Existing safety risk controls
- Triggering mechanisms
- Safety risk of reasonably likely outcomes from the existence of a hazard, to include estimation of the:
  - Likelihood
  - Severity

Element 2.2 - Risk Assessment and Control

Process 2.2.2 - Assess Safety Risk

Performance Objective:

The organization will assess risk associated with each identified hazard and define risk acceptance procedures and levels of management that can make safety risk acceptance decisions.

Design Expectations:

Each hazard will be assessed for its safety risk acceptability using the safety risk acceptance process described in Component 2.0 B).

Element 2.2 - Risk Assessment and Control

Process 2.2.3 - Control/Mitigate Safety Risk

Performance Objective:

The organization will design and implement a risk control for each identified hazard for which there is an unacceptable risk, to reduce to acceptable levels the potential for death, serious physical harm, or damage to equipment or property. The residual or substitute risk will be analyzed before implementing any risk control.

Design Expectations:

A. Safety control/mitigation plans will be defined for each hazard with unacceptable risk.

B. Safety risk controls will be:

- Clearly described
- Evaluated to ensure that the expectations have been met
- Ready to be used in their intended operational environment
- Documented

C. Substitute risk will be evaluated when creating safety risk controls/mitigations.

COMPONENT 3.0 - SAFETY ASSURANCE

Component Performance Objective:

The organization will monitor, measure, and evaluate the performance and effectiveness of risk controls.

Component General Design Expectations:

A. The organization will monitor their systems and operations to:

- Identify new hazards
- Measure the effectiveness of safety risk controls
- Ensure compliance with regulatory requirements applicable to the SMS
- Ensure that the safety assurance function is based upon a comprehensive system description as described in Process 2.1.1

B. The organization will collect the data necessary to demonstrate the effectiveness of its:

- Operational processes
- SMS

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.1 - Continuous Monitoring

Performance Objective:

The organization will monitor operational data, including products and services received from contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance.

Design Expectations:

A. The organization will monitor operational data (e.g., duty logs, crew reports, work cards, process sheets, and reports from the employee safety feedback system specified in Process 3.1.6) to:

- Determine conformity to safety risk controls (described in Process 2.2.3)
- Measure the effectiveness of safety risk controls (described in Process 2.2.3)
- Assess SMS system performance
- Identify hazards

B. The organization will monitor products and services received from subcontractors.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.2 - Internal Audits by Operational Departments

Performance Objective:

The organization will perform regularly scheduled internal audits of its operational processes, including those performed by contractors, to determine the performance and effectiveness of risk controls.

Design Expectations:

A. Line management of operational departments will conduct regular internal audits of safety-related functions of the organization's operational processes (production system). These audits will include any subcontractors who perform those functions.

NOTE: The internal audit is a primary means of output measurement under Component 1.0, C).

B. Line management will ensure that regular audits are conducted to:

- Determine conformity with safety risk controls
- Assess performance of safety risk controls

C. Planning of the audits program will take into account:

- Safety criticality of the processes to be audited
- The results of previous audits

D. The organization will define:

- Audits, including:
  - Criteria
  - Scope
  - Frequency

- Methods

• How they will select the auditors

• The requirement that auditors will not audit their own work

E. The organization will document audit procedures, to include:

• The responsibilities and expectations for:

- Planning audits
- Conducting audits
- Reporting results
- Maintaining records
- Auditing contractors and vendors

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.3 - Internal Evaluation

Performance Objective:

The organization will conduct internal evaluations of the SMS and operational processes at planned intervals to determine that the SMS conforms to its objectives and expectations.

Design Expectations:

A. The organization will conduct internal evaluations of the operational processes and the SMS at planned intervals to determine that the SMS conforms to objectives and expectations

NOTE: Sampling of SMS output measurement is a primary control under Component 1.0, C).

B. Planning of the evaluation program will take into account:

- Safety criticality of the processes being evaluated
- The results of previous evaluations

C. The organization will define:

- Evaluations, including:
  - o Criteria
  - o Scope
  - o Frequency
  - o Methods
- The processes used to select the evaluators

D. Documented procedures, which include:

- The responsibilities

- Requirements for:
    - o Planning evaluations
    - o Conducting evaluations
    - o Reporting results
    - o Maintaining records
    - o Evaluating contractors and vendors

E. The program will include an evaluation of the programs described in Component 1.0, B).

F. The person or organization performing evaluations of operational processes must be independent of the process being evaluated.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.4 - External Auditing of the SMS

Performance Objective:

The organization will include the results of assessments performed by oversight organizations in its analysis of data.

Design Expectations:

The organization will include the results of oversight organization assessments in the analyses conducted as described in Process 3.1.7.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.5 - Investigation

Performance Objective:

The organization will establish procedures to collect data and investigate incidents, accidents, and instances of potential regulatory non-compliance to identify potential new hazards or risk control failures.

Design Expectations:

A. The organization will collect data on:

- Incidents
- Accidents
- Real and potential regulatory non-compliance

B. The organization will establish procedures to:

- Investigate accidents
- Investigate incidents
- Investigate instances of real and potential regulatory non-compliance

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.6 - Employee Reporting and Feedback System

Performance Objective:

The organization will establish and maintain mandatory, voluntary and confidential safety reporting and feedback system. Data obtained from this system will be monitored to identify emerging hazards and to assess performance of risk controls in the operational systems.

Design Expectations:

A. The organization will establish and maintain mandatory, voluntary and confidential employee safety reporting and feedback system as in Component 4.0 B).

B. Employees will be encouraged to use the voluntary and confidential safety reporting and feedback system without fear of reprisal and to submit solutions/safety improvements where possible.

C. Data from the safety reporting and feedback system will be monitored to identify emerging hazards.

D. Data collected in the safety reporting and feedback system will be included in analyses described in Process 3.1.7.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.7 - Analysis of Data

Performance Objective:

The organization will analyze the data described in Processes 3.1.1 through 3.1.6 to assess the performance and effectiveness of risk controls in the organization's operational processes and the SMS, and to identify root causes of deficiencies and potential new hazards.

Design Expectations:

A. The organization will analyze the data described in Processes 3.1.1 through 3.1.6 to demonstrate the effectiveness of:

- Risk controls in the organization's operational processes
- The SMS

B. Through data analysis, the organization will evaluate where improvements can be made to the organizations:

- Operational processes
- The SMS

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.8 - System Assessment

Performance Objective:

The organization will perform an assessment of the performance and effectiveness of risk controls, conformance to SMS expectations as stated herein, and the objectives of the safety policy.

Design Expectations:

A. The organization will assess the performance of:

- Safety-related functions of operational processes against their objectives and expectations
- The SMS against its objective and expectations

B. System assessments will document results that indicate a finding of:

- Conformity with existing safety risk control(s)/SMS expectations(s) (including regulatory requirements)
- Nonconformity with existing safety risk control(s)/SMS expectations(s) (including regulatory requirements)
- New hazard(s) found

C. The SRM process will be utilized if the assessment indicates:

- The identification of new or potential hazards
- The need for system changes

D. The organization will maintain records of assessments in accordance with the expectations of Element 1.5.

Element 3.2 - Management of Change

Performance Objective:

The organization's management will identify and determine acceptable safety risk for changes within the organization that may affect established processes and services by new system design, changes to existing system designs, new operations/procedures, or modified operations/procedures.

Design Expectations:

A. The following will not be implemented until the safety risk of each identified hazard is determined to be acceptable in:

- New system designs
- Changes to existing system designs
- New operations/procedures
- Modified operations/procedures

B. The SRM process may allow an organization to take interim immediate action to mitigate existing safety risk.

Element 3.3 - Continual Improvement

Performance Objective:

The organization will promote continual improvement of its SMS through recurring application of Safety Risk Management (Component 2.0), Safety Assurance (Component 3.0), and by using safety lessons learned and communicating them to all personnel.

Design Expectations:

A. The organization will continuously improve SMS and safety risk control effectiveness through the use of the safety and quality policies, objectives, audit and evaluation results, analysis of data, corrective and preventive actions, and management reviews.

B. The organization will develop safety lessons learned.

1) Lessons learned information will be used to promote continuous improvement of safety; and

2) The organization will communicate information on safety lessons learned throughout the organization.

Element 3.3 - Continual Improvement

Process 3.3.1 - Preventive/Corrective Action

Performance Objective:

The organization will take corrective and preventive action to eliminate the causes of nonconformance identified during analysis, to prevent recurrence.

Design Expectations:

A. The organization will develop:

- Corrective actions for identified nonconformities with risk controls
- Preventive actions for identified potential nonconformities with risk controls

B. Safety lessons learned will be considered in the development of:

- Corrective actions
- Preventive actions

C. The organization will take necessary corrective and preventive action based on the findings of investigations.

D. The organization will prioritize and implement corrective and preventative action(s) in a timely manner.

E. Records will be kept and maintained of the disposition and status of corrective and preventive actions.

Element 3.3 - Continual Improvement

Process 3.3.2 - Management Review

Performance Objective:

Top management will conduct regular reviews of the SMS, including outputs of safety risk management, safety assurance, and lessons learned. Management reviews will include assessing the performance and effectiveness of an organization's operational processes and the need for improvements.

Design Expectations:

A. Top management will conduct regular reviews of the SMS, including:

- The outputs of safety risk management (Component 2.0)
- The outputs of safety assurance (Component 3.0)
- Lessons learned (Element 3.3, B)

B. Management reviews will include assessing the need for improvements to the organization's:

- Operational processes
- SMS

C. The organization will communicate information on safety lessons learned to all personnel.

COMPONENT 4.0 - SAFETY PROMOTION

General Performance Objective:

Top Management will promote the growth of a positive safety culture and communicate it throughout the organization.

Component General Design Expectations:

A. Top management will promote the growth of a positive safety culture by:

• Publication of senior management's stated commitment to safety to all employees

• Visibly demonstrating their commitment to the SMS

• Communicating the safety responsibilities for the organization's personnel

• Clearly and regularly communicating safety policy, goals, objectives, standards, and performance to all organizational employees

• Creating an effective employee reporting and feedback system that provides confidentiality, as needed

• Using a safety information system that provides an accessible, efficient means to retrieve safety information

• Making essential resources available to implement and maintain the SMS

Element 4.1 - Competencies and Training

Process 4.1.1 - Personnel Expectations (Competence)

Performance Objective:

The organization will document competency requirements for those positions identified in Element 1.2 C) and 1.3 and ensure those requirements are met.

Design Expectations:

A. The organization will determine and document competency requirements for those positions identified in Element 1.2 C) and 1.3.

B. The organization will ensure that those individuals in the positions identified in Element 1.2 C) and 1.3, meet the Process 4.1.1 A) competency requirements.

Element 4.1 - Competencies and Training

Process 4.1.2 - Training

Performance Objective:

The organization will develop, document, deliver, and regularly evaluate training necessary to meet competency requirements of 4.1.1.

Design Expectations:

A. Training needed to meet competency requirements of 4.1.1 will be developed for those individuals in the positions identified in Element 1.2 and 1.3.

B. Training development will consider scope, content, and frequency of training required to maintain competency for those individuals in the positions identified in Element 1.2 and 1.3.

C. Employees will receive training commensurate with their:

- Position level within the organization
- Impact on the safety of the organization’s products or services

D. To ensure training currency, it will be periodically:

- Reviewed
- Updated

Element 4.2 - Communication and Awareness

Performance Objective:

Top Management will communicate the outputs of its SMS to its employees, and will provide its oversight organization access to SMS outputs in accordance with established agreements and disclosure programs.

Design Expectations:

A. The organization will communicate outputs of the SMS to its employees.

B. The organization will provide its oversight organization access to the outputs of the SMS.

C. The organization's SMS will be able to inter-operate with other organizations' SMSs to cooperatively manage issues of mutual concern.

Component 1.0 - Safety Policy and Objectives

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• All levels of management clearly articulate the importance of safety when addressing company personnel

• Management has a clear commitment to safety and demonstrates it through active and visible participation in the safety management system

• Management makes the policy clearly visible to all personnel and particularly throughout the safety critical areas of the organization

• All personnel understand their authorities, responsibilities and accountabilities in regards to all safety management processes, decision and actions

• Safety objectives have been established utilizing a safety risk profile that considers hazards and risks

• Objectives and goals are consistent with the safety policy and their attainment is measurable.

• Safety objectives and goals are reviewed and updated periodically

• There is a documented process to develop a set of safety goals to achieve overall safety objectives

• Safety objectives and goals are documented and publicized

• There is controlled documentation that describes the SMS and the interrelationship between all of its elements

• Documentation is readily accessible to all personnel

• There is a process to periodically review SMS documentation to ensure its continuing suitability, adequacy and effectiveness, and that changes to company documentation have been implemented

Element 1.1 - Safety Policy

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• A safety policy is in existence, followed and understood

• The organization has based its safety management system on the safety policy and there is a clear commitment to safety

• The safety policy is agreed to and approved by the accountable executive

• The safety policy is promoted by the accountable executive

• The safety policy is reviewed periodically for continuing applicability

• The safety policy is communicated to all employees with the result that they are made aware of their safety obligations

• The policy is implemented at all levels of the organization

• *Safety objectives have been established utilizing a safety risk profile that considers hazards and risks*

• *Objectives and goals are consistent with the safety policy and their attainment is measurable.*

• *Safety objectives and goals are reviewed and updated periodically*

• There is a documented process to develop a set of safety goals to achieve overall safety objectives

• Safety objectives and goals are documented and publicized

• The organization has a process or system that provides for the capture of internal information including hazards, incidents and accidents and other data relevant to SMS

• The reactive reporting system is simple, accessible and commensurate with the size and complexity of the organization

• Reactive reports are reviewed at the appropriate level of management

• There is a feedback process to notify contributors that their reports have been received and to share the end results of the analysis

• The organization has a process in place to ensure confidentiality when requested

• The feedback process provides an opportunity for report submitters to indicate whether they are satisfied with the response

NOTE: The items above in *italics* are referring to the Safety Performance Indicators and Targets that require periodic review and agreement by GACA Inspectors as described in Section 4 of this Chapter. Further guidance on the periodic review of Safety Performance Indicators and Targets can also be found in Volume 12, Chapter 19.

Element 1.2 - Management Commitment and Safety Accountabilities

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• There are documented roles and responsibilities and accountabilities for the accountable executive and evidence that the SMS is established, maintained and adhered to

• Those management officials that can make safety risk management decisions are clearly identified, by position

• The accountable executive demonstrates control of the financial and human resources required for the proper execution of the SMS responsibilities

• Safety authorities, responsibilities and accountabilities are transmitted to all personnel

Element 1.3 - Key Safety Personnel

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• There are documented roles and responsibilities and accountabilities for the accountable executive to ensure the SMS is operating and maintained, and to keep top management informed of its continuing performance

• A qualified person has been appointed, in accordance with the regulation, and has demonstrated control of the SMS

• All personnel understand their authorities, responsibilities and accountabilities in regards to all safety management processes, decision and actions

Element 1.4 - Emergency Preparedness and Response

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• There is clear identification of who is responsible for the quality of the Emergency Preparedness and Response Process and associated documentation as well as the procedures and responsibilities for accomplishing the process

• There are clearly established emergency response procedures across all operational departments

• There is clearly established planning and execution of periodic exercises of the organization's emergency response procedures

• There is emergency preparedness and response training for affected personnel

Element 1.5 - SMS Documentation and Records

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• There is controlled documentation that describes the SMS and the interrelationship between all of its elements

• Documentation is readily accessible to all personnel

• There is a process to periodically review SMS documentation to ensure its continuing suitability, adequacy and effectiveness, and that changes to company documentation have been implemented

• The organization has a process to identify changes within the organization that could affect company documentation

Component 2.0 - Safety Risk Management

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this Component are obtained from the critical expectations of its systems and operational environment

• There is clear identification who is responsible for all aspects of the Safety Risk Management process

• The SMS includes, at a minimum, the following processes: System description and task analysis; Hazard identification; Safety risk analysis; Safety Risk assessment; and Safety risk control and mitigation

• The SMS processes apply to initial designs of systems, organizations and products, and to planned changes to operational processes

• There are feedback loops between assurance functions described in the Continuous Monitoring Process to evaluate the effectiveness of safety risk controls

• There are defined acceptable and unacceptable levels of safety risk

• There is defined acceptable risk for hazards that will exist in the short-term while safety risk control/mitigation plans are developed and implemented

Element 2.1 - Hazard Identification and Analysis

Process 2.1.1 System Description and Task Analysis

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for the System Description and Task Analysis process are obtained from the Safety Risk Management Component 2.0

• There are system descriptions and task analysis to the level of detail necessary to: Identify hazards; Develop operational procedures; and Develop and implement risk controls

Element 2.1 - Hazard Identification and Analysis

Process 2.1.2 - Identify Hazards

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for the Hazard Identification Process are obtained from the System Description and Task Analysis Process 2.1.1, to include a new hazard identified from the Safety Assurance Component 3.0, failures of risk controls due to design deficiencies found in the System Assessment Process 3.1.8 , and/or from any other source

• There is clear identification who is responsible for all aspects of the Hazard Identification process

• Hazards are identified for the entire scope of each system, as defined in the system description

• Identified hazards are tracked for the entire scope of each system, as defined in the system description

Element 2.2 Risk Assessment and Control

Process 2.2.1 Analyze Safety Risk

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the Hazard Identification Process 2.1.2

• There is clear identification who is responsible for all aspects of the Safety Risk Analysis process

• Safety risk analysis functions include: Analysis of existing safety risk controls; Triggering mechanisms; and, Safety risk of a reasonably likely outcome from the existence of a hazard

• Reasonably likely outcomes from the existence of a hazard, include estimations of the severity and likelihood

Element 2.2 Risk Assessment and Control

Process 2.2.2 Assess Safety Risk

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the Safety Risk Analysis Process 2.2.1 in terms of estimated severity and likelihood

• There is clear identification who is responsible for all aspects of the Safety Risk Assessment process

• Each hazard is analyzed for its safety risk acceptability using the safety risk acceptance process as described in Safety Risk Management Component 2.0

Element 2.2 Risk Assessment and Control

Process 2.2.3 Control/Mitigate Safety Risk

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for the Control/Mitigation Safety Risk process are obtained from the Safety Risk Assessment Process 2.2.2

• Residual risk is evaluated when creating safety risk controls and mitigations

• Interfaces between the risk control/mitigation functions (this process) and the Safety Assurance Component 3.0 are being identified and documented

• Performance objectives and design expectations of the risk Control/Mitigate Safety Risk Process are being reviewed periodically for successful accomplishment

COMPONENT 3.0 - SAFETY ASSURANCE

Component Performance Objective:

The organization will monitor, measure, and evaluate the performance and effectiveness of risk controls.

Component General Design Expectations:

A. The organization will monitor their systems and operations to:

- Identify new hazards
- Measure the effectiveness of safety risk controls
- Ensure compliance with regulatory requirements applicable to the SMS
- Ensure that the safety assurance function is based upon a comprehensive system description as described in Process 2.1.1

B. The organization will collect the data necessary to demonstrate the effectiveness of its:

- Operational processes
- SMS

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.1 - Continuous Monitoring

Performance Objective:

The organization will monitor operational data, including products and services received from contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance.

Design Expectations:

A. The organization will monitor operational data (e.g., duty logs, crew reports, work cards, process sheets, and reports from the employee safety feedback system specified in Process 3.1.6) to:

- Determine conformity to safety risk controls (described in Process 2.2.3)
- Measure the effectiveness of safety risk controls (described in Process 2.2.3)
- Assess SMS system performance
- Identify hazards

B. The organization will monitor products and services received from subcontractors.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.2 - Internal Audits by Operational Departments

Performance Objective:

The organization will perform regularly scheduled internal audits of its operational processes, including those performed by contractors, to determine the performance and effectiveness of risk controls.

Design Expectations:

A. Line management of operational departments will conduct regular internal audits of safety-related functions of the organization's operational processes (production system). These audits will include any subcontractors who perform those functions.

NOTE: The internal audit is a primary means of output measurement under Component 1.0, C).

B. Line management will ensure that regular audits are conducted to:

- Determine conformity with safety risk controls
- Assess performance of safety risk controls

C. Planning of the audits program will take into account:

- Safety criticality of the processes to be audited
- The results of previous audits

D. The organization will define:

- Audits, including:
  - Criteria
  - Scope
  - Frequency

- Methods

• How they will select the auditors

• The requirement that auditors will not audit their own work

E. The organization will document audit procedures, to include:

• The responsibilities and expectations for:

- Planning audits
- Conducting audits
- Reporting results
- Maintaining records
- Auditing contractors and vendors

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.3 - Internal Evaluation

Performance Objective:

The organization will conduct internal evaluations of the SMS and operational processes at planned intervals to determine that the SMS conforms to its objectives and expectations.

Design Expectations:

A. The organization will conduct internal evaluations of the operational processes and the SMS at planned intervals to determine that the SMS conforms to objectives and expectations

NOTE: Sampling of SMS output measurement is a primary control under Component 1.0, C).

B. Planning of the evaluation program will take into account:

- Safety criticality of the processes being evaluated
- The results of previous evaluations

C. The organization will define:

- Evaluations, including:
  - o Criteria
  - o Scope
  - o Frequency
  - o Methods
- The processes used to select the evaluators

D. Documented procedures, which include:

- The responsibilities

- Requirements for:
    - o Planning evaluations
    - o Conducting evaluations
    - o Reporting results
    - o Maintaining records
    - o Evaluating contractors and vendors

E. The program will include an evaluation of the programs described in Component 1.0, B).

F. The person or organization performing evaluations of operational processes must be independent of the process being evaluated.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.4 - External Auditing of the SMS

Performance Objective:

The organization will include the results of assessments performed by oversight organizations in its analysis of data.

Design Expectations:

The organization will include the results of oversight organization assessments in the analyses conducted as described in Process 3.1.7.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.5 - Investigation

Performance Objective:

The organization will establish procedures to collect data and investigate incidents, accidents, and instances of potential regulatory non-compliance to identify potential new hazards or risk control failures.

Design Expectations:

A. The organization will collect data on:

- Incidents
- Accidents
- Real and potential regulatory non-compliance

B. The organization will establish procedures to:

- Investigate accidents
- Investigate incidents
- Investigate instances of real and potential regulatory non-compliance

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.6 - Employee Reporting and Feedback Systemv

Performance Objective:

The organization will establish and maintain mandatory, voluntary and confidential safety reporting and feedback system. Data obtained from this system will be monitored to identify emerging hazards and to assess performance of risk controls in the operational systems.

Design Expectations:

A. The organization will establish and maintain mandatory, voluntary and confidential employee safety reporting and feedback system as in Component 4.0 B).

B. Employees will be encouraged to use the voluntary and confidential safety reporting and feedback system without fear of reprisal and to submit solutions/safety improvements where possible.

C. Data from the safety reporting and feedback system will be monitored to identify emerging hazards.

D. Data collected in the safety reporting and feedback system will be included in analyses described in Process 3.1.7.

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.7 - Analysis of Data

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the data acquisition processes 3.1.1 through 3.1.6

• There is clear identification who is responsible for all aspects of the Analysis of Data Process

• There are procedures in place to analyze the data collected to demonstrate the effectiveness of the following: Risk controls in the organization's operational processes (SMS Framework Safety Policy Component; and, the Service Provider SMS

• There are procedures in place to analyze the data collected to identify root causes of deficiencies and potential new hazards and evaluate where improvements can be made in the following: Operational processes (SMS Framework Safety Policy Component); and, the Service Provider SMS

• Performance objectives and design expectations of the Analysis of Data Process are being reviewed periodically for successful accomplishment

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.8 - System Assessment

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the Analysis of Data Process 3.1.7

• There is clear identification who is responsible for all aspects of the System Assessment Process

• There are procedures in place, and conducted, to assess the performance and effectiveness of the following: Safety-related functions of operational processes (Safety Policy Component) against their requirements; and, the SMS against its objectives and expectations

• There are procedures in place, and conducted, to record system assessments that result in a finding of the following: Conformity or nonconformity with existing safety risk controls and/or SMS expectations, including regulatory requirements; and, New hazards found

• There are procedures in place, and conducted, to use the Safety Risk Management (Component 2.0) if risk assessment and risk control performance indicates the following: That new hazards or potential hazards have been found; and/or, That the system needs to be changed

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the System Assessment Process

Element 3.2 - Management of Change

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from proposed changes to systems, processes, procedures, or organizational structures

• There is clear identification who is responsible for all aspects of the Management of Change Process

• There are requirements and procedures in place to not implement any of the following until the level of safety risk of each identified hazard is determined to be acceptable for: New system designs; Changes to existing system designs; New operations or procedures; and, Modifications to existing operations or procedures

• Performance objectives and design expectations of the Management of Change Process are being reviewed periodically for successful accomplishment

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Management of Change Process

Element 3.3 Continuous Improvement

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained through continuous application of Safety Risk Management (Component 2.0), Safety Assurance (Component 3.0) and the outputs of the SMS, including safety lessons learned

• There is clear identification who is responsible for all aspects of the Continuous Improvement Process

• There are requirements and procedures in place to continuously improve the effectiveness of the SMS and of safety risk controls through the use of the safety and quality policies, objectives, audit and evaluation results, analysis of data, corrective and preventive actions, and management reviews

• Performance objectives and design expectations of the Continuous Improvement Process are being reviewed periodically for successful accomplishment

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Continuous Improvement Process

Element 3.3 Continuous Improvement

Process 3.3.1 Preventive/Corrective Action

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from System Assessments (Process 3.1.8) with findings of non-performing risk controls

• There is clear identification who is responsible for all aspects of the Preventive/Corrective Action Process

• There is a requirement and documented action to develop the following: Preventive actions for identified potential nonconformities with risk controls; and, Corrective actions for identified nonconformities with risk controls

• There is a requirement and documented action to consider safety lessons learned in the development of both preventive actions and corrective actions

• There is a requirement and documented action to take necessary preventive and corrective action based on the findings of investigations

• There is a requirement and documented action to prioritize and implement preventive and corrective actions in a timely manner

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Preventive/Corrective Action Process

Element 3.3 Continuous Improvement

Process 3.3.2 - Management Review

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the outputs of Safety Risk Management (Component 2.0) and Safety Assurance (Component 3.0) activities

• There is clear identification who is responsible for all aspects of the Management Review Process

• Top management conducts regular reviews of the SMS, including the outputs of the Safety Risk Management Processes, the outputs of the Safety Assurance Processes, and safety lessons learned

• Top management includes in its reviews of the SMS, an assessment of the need for improvements to the organization's operational processes and the SMS

• There is a requirement and action to keep records of the disposition and status of management reviews according to the organization's record retention policy

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Management Review Process

Component 4.0 - Safety Promotion

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) are identified between top management and organizational personnel

• There is clear identification who is responsible for all aspects of the Safety Promotion Component 4.0

•Top management promotes the growth of a positive safety culture through the following: Publication of top management's stated commitment to safety to all employees; Visible demonstration of their commitment to the SMS; Communication of the safety responsibilities for the organization's personnel; Clear and regular communication of safety policy, goals, expectations, standards, and performance to all employees of the organization; An effective employee reporting and feedback system that provides confidentiality; Use of a safety information system that provides an accessible efficient means to retrieve information; and, Allocation of resources essential to implement and maintain the SMS

• Performance objectives and design expectations of the Safety Promotion Component are being reviewed periodically for successful accomplishment

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Safety Promotion Component

Element 4.1 Competencies and Training

Process 4.1.1 - Personnel Expectations (Competence)

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are identified between top management and the key safety personnel referenced in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3

• There is clear identification who is responsible for all aspects of the Personnel Expectations Process

• There is a requirement and action to identify the competency requirements for safety-related positions identified in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3

• There is a requirement and action to ensure that the personnel in the safety-related positions identified in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3 meet the documented competency requirements of Personnel Expectations Process 4.1.1

• Performance objectives and design expectations of the Personnel Expectations Process are being reviewed periodically for successful accomplishment

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Personnel Expectations Process

Element 4.1 Competencies and Training

Process 4.1.2 – Training

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for the Training Process are obtained through the outputs of the SMS and the documented competency expectations of Personnel Expectations Process

• There is clear identification who is responsible for all aspects of the SMS Training Process

• There is implemented training to meet the competency expectations of Personnel Expectations Process 4.1.1 for the personnel in the safety-related positions identified in Management Commitment and Safety Accountability Element 1.2 & Key Safety Personnel Element 1.3

• There is a requirement and action to consider scope, content, and frequency of training required to meet and maintain competency for those individuals in the positions identified in Management Commitment and Safety Accountability Element 1.2 and Key Safety Personnel 1.3

• Employees receive training commensurate with their: Position level within the organization; and, Impact on the safety of the organization’s products or services

• There is a requirement and action to maintain training currency by periodically reviewing training and updating the training

• There is a requirement and action to maintain records of required and delivered training

• Safety-related training media is periodically reviewed and updated for target populations

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the SMS Training Process

Element 4.2 - Communication and Awareness

Acceptance Criteria:

Evidence of acceptable component and element content and/or activity includes the following:

• Inputs (interfaces) for this process are obtained from the outputs of Safety Risk Management Component 2.0 and Safety Assurance Component 3.0

• There is clear identification who is responsible for all aspects of the Communication and Awareness Process

• There is a requirement and action to communicate outputs of the SMS, rationale behind controls, preventive and corrective actions and ensure awareness of SMS objectives to its employees

• There is a requirement and action in place to provide it's the GACA access to the outputs of the SMS in accordance with established agreements and disclosure programs

• There is interface with other organizations' SMSs to cooperatively manage issues of mutual concern

• Performance objectives and design expectations of the Communication and Awareness Process are being reviewed periodically for successful accomplishment

• There is periodic review of supervisory and operational controls to ensure the effectiveness of the Communication and Awareness Process

APPENDIX C - SMS ASSESSMENT GUIDE

Component 1.0 - Safety Policy and Objectives

Component Performance Objective:

The organization will develop and implement an integrated, comprehensive SMS for its organization and will incorporate a procedure to identify and maintain compliance with all applicable regulatory statutory requirements.

Design Expectations
Management Accountability
Does the organization clearly identify who is responsible for the quality of the organizational management processes (name, position, organization)? Do procedures will also define who is responsible for accomplishing the process?
Procedure: Scope
Does the organization's SMS include the complete scope and life cycle of the organization's systems?
Procedure: Management
Does the organization require the SMS processes to be -
• Documented?
• Monitored?
• Measured?
• Analyzed?
Procedure: Promotion of Positive Safety Culture
Does the organization promote a positive safety culture as in Safety Promotion Component 4.0?
Procedure: Quality Policy
Does top management ensure that the organization's quality policy, if present, is consistent with (or not in conflict with) it's SMS?

Procedure: Safety Management Planning
Does the organization establish and maintain measurable criteria that accomplish the objectives of its Safety Policy?
Does the organization establish and maintain a safety management plan to describe methods for achieving the safety objectives set forth in its Safety Policy?
Procedure: Regulatory Compliance
Does the organization identify all current and forthcoming GACA regulatory requirements?
Does the organization ensure the SMS complies with all applicable regulatory requirements?
Outputs and Measures
Does the organization ensure all SMS outputs are -
• Recorded?
• Monitored?
• Measured?
• Analyzed?
Does the organization periodically measure performance objectives and design expectations of the general Safety Policy Component?
Controls
Does the organization establish and maintain supervisory and operational controls to ensure procedures are followed for safety-related operations and activities?

Bottom Line Assessment:

Has the organization developed and implemented an integrated, comprehensive SMS for its entire organization and incorporated a procedure to identify and maintain compliance with current safety-related, regulatory, and other requirements?

Element 1.1 - Safety Policy

Performance Objective:

Top management will define the organization's Safety Policy and convey its expectations and objectives to its employees.

Design Expectations
Management Accountability
Does top management define the organization's Safety Policy?
Procedure
Does the organization's Safety Policy include the following -
• A commitment to implement and maintain the SMS?
• A commitment to continuously improve the level of safety?
• A commitment to managing safety risk?
• A commitment to comply with all applicable regulatory requirements?
• A commitment to encourage employees to report safety issues without reprisal, as per SMS Framework Employee Reporting and Feedback System Process 3.1.6?
• Clear standards for acceptable behavior for all employees?
Is the Safety Policy documented?
Outputs and Measures
Does the Safety Policy provide guidance to management on setting safety objectives?
Does the Safety Policy provide guidance to management on reviewing safety objectives?
Does the organization ensure the Safety Policy is communicated, with visible management endorsement, to all employees and responsible parties?
Does the organization ensure the Safety Policy is reviewed periodically to verify it remains relevant and appropriate to the organization?
Does the organization identify and communicate management and individuals' safety performance responsibilities?
The organization will periodically measure performance objectives and design expectations of the Safety Policy Element.

Bottom Line Assessment:

Has top management defined the organization's Safety Policy and conveyed the expectations and objectives of that policy to its employees?

Element 1.2 - Management Commitment and Safety Accountabilities

Performance Objective:

The organization will define, document, and communicate the safety roles, responsibilities, and authorities throughout its organization.

Design Expectations
Management Accountability
Does the organization ensure top management has the ultimate responsibility for the SMS?
Does the organization's top management provide the resources needed to implement and maintain the SMS?
Does the organization define levels of management that can make safety risk acceptance decisions as described in Component 2.0, D)?
Procedure/Output/Measure
Does the organization ensure that aviation safety-related positions, responsibilities, and authorities are -
• Defined?
• Documented?
• Communicated throughout the organization?
Does the organization periodically measure performance objectives and design expectations of the Management Commitment and Safety Accountabilities Element?

Bottom Line Assessment:

Has the organization defined, documented, and communicated the safety roles, responsibilities, and authorities throughout the organization?

Element 1.3 - Key Safety Personnel

Performance Objective:

The organization will appoint a safety manager to manage, monitor and coordinate the SMS processes throughout its organization.

Design Expectations
Management Responsibility/Procedure
Did top management appoint a member of management who, irrespective of other responsibilities, will be responsible for and authorized to -
• Ensure that SMS processes are established, implemented, and maintained?
• Report to top management on the performance of the SMS and what needs to be improved?
• Ensure the organization communicates its safety requirements throughout the organization?
Outputs and Measures
Does the organization ensure that Key Safety Personnel positions, responsibilities, and authorities are communicated throughout the organization?
The organization will periodically measure performance objectives and design expectations of the Key Safety Personnel Element 1.3.

Bottom Line Assessment:

Has the organization appointed a safety manager to manage, monitor and coordinate the SMS processes throughout its organization?

Element 1.4 - Emergency Preparedness and Response

Performance Objective:

The organization will develop and implement procedures that it will follow in the event of an accident, incident or operational emergency to mitigate the effects of these events.

Design Expectations
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Emergency Preparedness and Response Process and associated documentation? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization establish procedures across all operational departments as expected in Safety Policy and Objectives Component 1.0 to -
• Identify hazards which have potential for accidents, incidents or operational emergencies?
• Coordinate and plan the organization's response to accidents, incidents or operational emergencies?
• Execute periodic exercises of the organization's emergency response procedures?
Outputs and Measures
Does the organization: • Identify interfaces between the emergency response functions of different operational elements of the organization?; and • Periodically measure performance objectives and design expectations of the Emergency Preparedness and Response Element?

Bottom Line Assessment:

Has the organization developed and implemented procedures that it will follow in the event of an accident, incident or operational emergency to mitigate the effects of these events?

Element 1.5 - SMS Documentation and Records

Performance Objective:

The organization will have documented safety policies, objectives, procedures, a document/record management process, and a management plan that meet organizational safety expectations and objectives.

Design Expectations
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Documentation and Records Process? Do procedures define who is responsible for accomplishing the process?
Procedure: Document Contents
Does the organization establish and maintain, in paper or electronic format, information to describe the following -
• Safety policies?
• Safety objectives?
• SMS expectations?
• Safety procedures and processes?
• Accountabilities, responsibilities and authorities for safety-related procedures and processes?
• Interactions and interfaces between safety-related procedures and policies?
• SMS outputs?
Procedure: Document Quality
Does the organization require all documentation be -
• Legible?
• Dated (with the dates of revisions)?
• Readily identifiable?
• Maintained in an orderly manner?
• Retained for a specified period as determined by the organization?

Procedure: Document Management
Does the organization control all documents to ensure -
• They are easily located?
• They are periodically reviewed?
• They are revised as needed?
• Authorized personnel approve them for adequacy?
Does the organization ensure that all current document versions are available at all locations where essential SMS operations are performed?
Does the organization ensure that obsolete documents are either removed as soon as possible, or that they are not used accidentally?
Outputs and Measures
Has the organization maintained their safety management plan in accordance with the objectives and expectations contained within this Element?
Does the organization ensure SMS records are -
• Identified?
• Maintained?
• Disposed of?
• Legible?
• Easy to identify?
• Traceable to the activity involved?
• Easy to find?
• Protected against damage?
• Protected against deterioration?
• Protected against loss?
• Annotated with record retention times?
Does the organization periodically measure performance objectives and design expectations of the Documentation and Records Element?

Bottom Line Assessment:

Has the organization clearly defined and documented (in paper or electronic format) safety policies, objectives, procedures, and document/record maintenance processes and established, implemented, and maintained a safety management plan that meets the safety expectations and objectives?

Component 2.0 - Safety Risk Management

Component Performance Objective

The organization will develop processes to understand the critical characteristics of its systems and operational environment and apply this knowledge to identify hazards, analyze and assess risk and design risk controls.

Component General Design Expectations
Input
Does the organization identify inputs (interfaces) for this Component obtained from the critical expectations of its systems and operational environment?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Risk Management Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization's SMS, at a minimum, include the following processes -
• System description and task analysis?
• Hazard Identification?
• Safety Risk Analysis?
• Safety Risk Assessment?
• Safety Risk Control and Mitigation?
Does the organization's SMS processes apply to -
• Initial designs of systems, organizations, and/or products?
• Hazards that are identified in the safety assessment functions (described in Safety Assurance Component 3.0?
• Planned changes to operational processes?
Does the organization establish feedback loops between assessment functions described in the Continuous Monitoring Process 3.1.1 to evaluate the effectiveness of safety risk controls?
Does the organization define acceptable and unacceptable levels of safety risk (for example, does the organization have a safety risk matrix)?

Does the organization's safety risk acceptance process include descriptions of the following -
• Severity levels?
• Likelihood levels?
• Level of management that can make safety risk acceptance decisions in accordance with Element 1.2?
Does the organization define acceptable risk for hazards that will exist in the short-term while safety risk control/mitigation plans are developed and implemented?
Outputs and Measures
Does the organization:
• Identify interfaces between the Safety Risk Management Component (this Component) and the Safety Assurance Component (3.0)?; and • Periodically measure performance objectives and design expectations of the safety risk management component?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?;and • They periodically review supervisory and operational controls to ensure the effectiveness of the Safety Risk Management Component (2.0)?

Bottom Line Assessment:

Has the organization developed processes to understand the critical characteristics of its systems and operational environment and applied this knowledge to the identification of hazards, risk analysis and risk assessment, and the design of risk controls?

Element 2.1 - Hazard Identification and Analysis

Process 2.1.1 System Description and Task Analysis

Performance Objective:

The organization will describe and analyze its systems, operations, and operational environment to gain an understanding of critical design and performance factors, processes, and activities to identify hazards.

Design Expectations
Input
Are inputs (interfaces) for the System Description and Task Analysis process obtained from the Safety Risk Management Component 2.0?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the System Description and Task Analysis Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization develop system descriptions and task analysis to the level of detail necessary to -
• Identify hazards?
• Develop operational procedures?
• Develop and implement risk controls?
Outputs and Measures
Does the organization: • Identify interfaces between the system description and task analysis function (this process) and the Hazard Identification Process 2.1.2 below?, and • Periodically measure performance objectives and design expectations of the System Description and Task Analysis Process (2.1.1)?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the System Description and Task Analysis Process (2.1.1)?

Bottom Line Assessment:

Has the organization analyzed its systems, operations and operational environment to gain an understanding of critical design and performance factors, processes, and activities to identify hazards?

Element 2.1 - Hazard Identification and Analysis

Process 2.1.2 - Identify Hazards

Performance Objective:

The organization will identify and document the hazards in its operations that are likely to cause death, serious physical harm, or damage to equipment or property in sufficient detail to determine associated level of risk and risk acceptability.

Design Expectations
Input
Are inputs (interfaces) for the Hazard Identification Process obtained from the System Description and Task Analysis Process 2.1.1, to include a new hazard identified from the Safety Assurance Component 3.0, failures of risk controls due to design deficiencies found in the System Assessment Process 3.1.8 and/or from any other source?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Hazard Identification Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization identify hazards for the entire scope of each system, as defined in the system description? **Note:** While it is recognized that identification of every conceivable hazard is impractical, aviation service providers are expected to exercise due diligence in identifying and controlling significant and reasonably foreseeable hazards related to their operations.
Does the organization document the identified hazards?
Does the organization have a means of tracking hazard information?
Does the organization manage hazard information through the entire Safety Risk Management Process?
Outputs and Measures
Does the organization: • Identify interfaces between this process and the Analysis of Safety Risk Process (2.2.1, below)?, and • Periodically measure performance objectives and design expectations of the Hazard Identification Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Hazard Identification Process?

Bottom Line Assessment:

Has the organization identified and document the hazards in its operations that are likely to cause death, serious physical harm, or damage to equipment or property in sufficient detail to determine associated level of risk and risk acceptability?

Element 2.2 Risk Assessment and Control

Process 2.2.1 Analyze Safety Risk

Performance Objective:

The organization will determine and analyze the severity and likelihood of potential events associated with identified hazards and will identify risk factors associated with unacceptable levels of severity or likelihood.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Hazard Identification Process (2.1.2)?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Risk Analysis Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization's safety risk analysis functions include -
• Analysis of existing safety risk controls?
• Triggering mechanisms?
• Safety risk of a reasonably likely outcome from the existence of a hazard?
Does the organization's reasonably likely outcomes from the existence of a hazard, include estimations of the following -
• Likelihood?
• Severity?
Outputs and Measures
Does the organization: • Identify interfaces between the risk analysis functions (this process) and the Risk Assessment Process 2.2.2, below)?, and • Periodically measure performance objectives and design expectations of the Risk Analysis Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Analysis of Safety Risk Process?

Bottom Line Assessment:

Has the organization determined and analyzed the factors related to the severity and likelihood of potential events associated with identified hazards and identified factors associated with unacceptable levels of severity or likelihood?

Element 2.2 Risk Assessment and Control

Process 2.2.2 Assess Safety Risk

Performance Objective:

The organization will assess risk associated with each identified hazard and define risk acceptance procedures and levels of management that can make safety risk acceptance decisions.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Safety Risk Analysis Process 2.2.1 in terms of estimated severity and likelihood?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Risk Assessment Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization analyze each hazard for its safety risk acceptability using their safety risk acceptance process as described in the SMS Framework Safety Risk Management Component 2.0?
Outputs and Measures
Does the organization: • Identify interfaces between the risk assessment functions (this process) and the Control/Mitigate Safety Risk Process 2.2.3. below?, and • Periodically measure performance objectives and design expectations of the Safety Risk Assessment Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Safety Risk Assessment Process?.

Bottom Line Assessment:

Has the organization assessed risk associated with each identified hazard and defined risk acceptance procedures and levels of management that can make safety risk acceptance decisions?

Element 2.2 Risk Assessment and Control

Process 2.2.3 Control/Mitigate Safety Risk

Performance Objective:

The organization will design and implement a risk control for each identified hazard for which there is an unacceptable risk, to reduce risk to acceptable levels. The potential for residual risk and substitute risk will be analyzed before implementing risk controls.

NOTE: Although Process 2.2.3 is very similar to the Preventive/Corrective Action Process 3.3.1, the primary differences are:

- Process 2.2.3 is used during the design of a system (often looking to the future) or in the redesign of a non-performing system where system requirements are being met, however the system is not producing the desired results.

- Process 2.2.3 is also used when new hazards are discovered during the safety assessment process that was not taken into account during initial design.

- Process 3.3.1 is used to develop actions to bring a non-performing system back into conformance to its design requirements.

Design Expectations
Input
Are inputs (interfaces) for the System Description and Task Analysis process obtained from the Safety Risk Management Component 2.0?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the System Description and Task Analysis Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization develop system descriptions and task analysis to the level of detail necessary to -
• Identify hazards?
• Develop operational procedures?
• Develop and implement risk controls?
Outputs and Measures
Does the organization: • Identify interfaces between the system description and task analysis function (this process) and the Hazard Identification Process 2.1.2 below?, and • Periodically measure performance objectives and design expectations of the System Description and Task Analysis Process (2.1.1)?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the System Description and Task Analysis Process (2.1.1)?

Bottom Line Assessment:

Has the organization designed and implemented a risk control for each identified hazard for which there is unacceptable risk, to reduce to acceptable levels the potential for death, serious physical harm, or damage to equipment or property? Has the residual or substitute risk been analyzed before implementing any risk control?

COMPONENT 3.0 - SAFETY ASSURANCE

Component Performance Objective:

The organization will monitor, measure, and evaluate the performance of their systems to identify new hazards, measure the effectiveness of risk controls, (to include preventative and corrective actions) and ensure compliance with regulatory requirements.

Component Design Expectations
Input
Are inputs (interfaces) for this component will be obtained from the Safety Risk Management Component 2.0?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Assurance Component? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization monitor their systems and operations to: • Identify new hazards? • Measure the effectiveness of safety risk controls? • Ensure compliance with regulatory requirements applicable to the SMS?
Is the organization's safety assessment function based upon a comprehensive system description and task analysis as described in Process 2.1.1, System Description and Task Analysis? Does the organization collect the data necessary to demonstrate the effectiveness of its – • Operational processes? • The SMS?

Outputs and Measures
• Does the organization identify interfaces between the data acquisition processes (3.1.1 to 3.1.6) and the system assessment process (2.2.2)? • The hazard identification process (2.1.2)? Does the organization periodically measure performance objectives and design expectations of the Safety Assurance Component?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Safety Assurance Component?

Bottom Line Assessment:

Has the organization monitored, measured, and evaluated the performance of their systems to identify new hazards, measure the effectiveness of risk controls, (to include preventative and corrective actions) and ensured compliance with regulatory requirements?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.1 - Continuous Monitoring

Performance Objective:

The organization will monitor operational data, including products and services received from contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Risk Assessment Process 2.2.2, Risk Control/Mitigation Process 2.2.3, System Assessment Process 3.1.8 or Preventive/Corrective Action Process 3.3.1?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Continuous Monitoring Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization monitor operational data (e.g., duty logs, crew reports, work cards, process sheets, and reports from the employee safety feedback system specified in Process 3.1.6) to:
• Determine whether it conforms to safety risk controls (described in Process 2.2.3)?
• Measure the effectiveness of safety risk controls (described in Process 2.2.3)?
• Assess SMS system performance?
• Identify hazards?
Does the organization monitor products and services from contractors?
Outputs and Measures
Does the organization:
• Identify interfaces between these continuous monitoring functions and the Analysis of Data Process 3.1.7 below?, and • Periodically measure performance objectives and design expectations of the Continuous Monitoring Process?

Bottom Line Assessment:

Has the organization monitored operational data, including products and services received from contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.2 - Internal Audits by Operational Departments

Performance Objective:

The organization will perform regularly scheduled internal audits of its operational processes, including those performed by contractors, to verify safety performance and evaluate the effectiveness of safety risk controls.

Design Expectations
Input
Are inputs (interfaces) for this component obtained from the Safety Risk Management Component 2.0?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Assurance Component? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization monitor their systems and operations to:
• Identify new hazards?
• Measure the effectiveness of safety risk controls?
• Ensure compliance with regulatory requirements applicable to the SMS?
Is the organization's safety assessment function based upon a comprehensive system description and task analysis as described in Process 2.1.1?
Does the organization collect the data necessary to demonstrate the effectiveness of its -
• Operational processes?
• The SMS?

Outputs and Measures
Does the organization identify interfaces between the data acquisition processes (3.1.1 to 3.1.6) and:
• The system assessment process (2.2.2)?
• The hazard identification process (2.1.2)?
Does the organization periodically measure performance objectives and design expectations of the Safety Assurance Component? *See note at 3.1.3*
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Safety Assurance Component?

Bottom Line Assessment

Has the organization monitored operational data, including products and services received from contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.3 - Internal Evaluation

Performance Objective:

The organization will conduct internal evaluations of the SMS and operational processes at planned intervals to determine that the SMS conforms to its objectives and expectations.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Risk Assessment Process 2.2.2 or Control/Mitigate Safety Risk Process 2.2.3?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Internal Evaluation Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization ensure internal evaluations of operational processes and the SMS are conducted at planned intervals, to determine that the SMS conforms to objectives and expectations? **Note:** Sampling of SMS output measurement is a primary control under Component 1.0.
Does the organization's planning of the internal evaluation program take into account -
• Safety criticality of the processes being evaluated?
• Results of previous evaluations?
Procedure: Program Contents
Does the organization define what an evaluation is?
Does the definition for evaluations include information about evaluation -
• Criteria?
• Scope?
• Frequency?
• Methods?
• Processes used to select the evaluators?

Procedure: Documentation
Does the organization's document procedures include -
• Evaluation responsibilities?
• Requirements for -
• Planning evaluations?
• Conducting evaluations?
• Reporting results?
• Maintaining records?
• Evaluating contractors and vendors?
Procedure: Scope
Does the organization's evaluation program include an evaluation of the operational departments described in SMS Framework Safety Policy Component 1.0?
Procedure: Independence of Evaluators
Does the organization ensure the person or organization performing evaluations of operational processes are independent of the process being evaluated?
Outputs and Measures
Does the organization: • Identify interfaces between this process and the Analysis of Data Process 3.1.7 below?, and • Periodically measure performance objectives and design expectations of the Internal Evaluation Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Internal Evaluation Process?

Bottom Line Assessment:

Has the organization conducted internal evaluations of the SMS and operational processes at planned intervals to determine that the SMS conforms to its objectives and expectations?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.4 - External Auditing of the SMS

Performance Objective:

The organization will include the results of assessments performed by oversight organizations, and other external audit results, in its data analysis.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Control/Mitigate Safety Risk Process 2.2.3 and from the GACA and/or other external agencies?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the External Auditing Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization ensure it includes the results of oversight organization audits, and other external audit results, in the analyses conducted under SMS Framework Analysis of Data Process 3.1.7?
Outputs and Measures
The organization will: • Identify interfaces between this process and the Analysis of Data Process 3.1.7 below?, and • Periodically measure performance objectives and design expectations of the External Auditing Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the External Auditing Process?

Bottom Line Assessment:

Has the organization included the results of audits performed by oversight organizations, and other external audit results, in its analysis of data?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.5 - Investigation

Performance Objective:

The organization will establish procedures to collect data and investigate incidents, accidents, and instances of potential regulatory non-compliance to identify potential new hazards or risk control failures.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Control/Mitigate Safety Risk Process 2.2.3 and as needed upon occurrence of events?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Investigation Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization ensure it collects data on -
• Incidents?
• Accidents?
• Potential regulatory non-compliance?)
Does the organization ensure that procedures are established to investigate -
• Accidents?
• Incidents?
• Instances of potential regulatory non-compliance?
Outputs and Measures
Does the organization: • Identify interfaces between this process and the Analysis of Data Process 3.1.7 below? and • Periodically measure performance objectives and design expectations of the Investigation Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Investigative Process?

Bottom Line Assessment:

Has the organization established procedures to collect data and investigate incidents, accidents, and instances of potential regulatory non-compliance that occur to identify potential new hazards or risk control failures?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.6 - Employee Reporting and Feedback System

Performance Objective:

The organization will establish and maintain mandatory, voluntary and confidential Employee Safety Reporting and Feedback Systems. Data obtained from this system will be monitored to identify emerging hazards and to assess performance of risk controls in the operational systems.

Design Expectations
Input
Are inputs (interfaces) for the Employee Reporting and Feedback System obtained from employees?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Employee Reporting and Feedback Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Has the organization established and maintained a mandatory, voluntary and a confidential Employee Reporting and Feedback System as in the Safety Promotion component?
Does the organization ensure employees are encouraged to use the Safety Reporting and Feedback Systems without fear of reprisal and to encourage submission of solutions/safety improvements where possible?
Does the organization ensure data from the Safety Reporting and Feedback System is monitored to identify emerging hazards?
Does the organization ensure the data collected in the Employee Reporting and Feedback System is included in the analyses conducted under SMS Framework Analysis of Data Process 3.1.7?
Outputs and Measures
Does the organization: • Identify interfaces between this process and the Analysis of Data Process 3.1.7 below? and • Periodically measure performance objectives and design expectations of the Employee Reporting and Feedback Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Employee Reporting and Feedback Process?

Bottom Line Assessment:

Has the organization established and maintained a Confidential Employee Safety Reporting and Feedback System? Are the data obtained from this system monitored to identify emerging hazards and to assess performance of risk controls in the operational systems?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.7 - Analysis of Data

Performance Objective:

The organization will analyze the data described in SMS Framework Processes 3.1.1 through 3.1.6, to assess the risk controls' performance and effectiveness in the organization's operational processes and the SMS, and to identify root causes of deficiencies and potential new hazards.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the data acquisition processes 3.1.1 through 3.1.6?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Analysis of Data Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization analyze the data that it collects to demonstrate the effectiveness of -
• Risk controls in the organization's operational processes (SMS Framework Safety Policy Component?
• The organization's SMS?
Does the organization ensure it analyzes the data it collects to identify root causes of deficiencies and potential new hazards and evaluate where improvements can be made in the organization's -
• Operational processes (SMS Framework Safety Policy Component?
• The SMS?
Outputs and Measures
Does the organization: • Identify interfaces between this process and the System Assessment Process 3.1.8 below? and • Periodically measure performance objectives and design expectations of the Analysis of Data Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Analysis of Data Process?

Bottom Line Assessment:

Has the organization analyzed the data described in SMS Framework Processes 3.1.1 through 3.1.6 to assess the risk controls' performance and effectiveness in the organization's operational processes and the SMS and to identify root causes of deficiencies and potential new hazards?

Element 3.1 - Safety Performance Monitoring and Measurement

Process 3.1.8 - System Assessment

Performance Objective:

The organization will perform an assessment of the safety performance and effectiveness of risk controls, conformance to SMS expectations as stated herein, and the objectives of the safety policy.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the Analysis of Data Process 3.1.7.
Management Responsibility
Does the organization will clearly identify who is responsible for the quality of the System Assessment Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization assess the performance and effectiveness of the -
• Safety-related functions of operational processes (Safety Policy Component) against their requirements?
• SMS against its objectives and expectations?
Does the organization record system assessments that result in a finding of -
• Conformity or nonconformity with existing safety risk controls and/or SMS expectations, including regulatory requirements?
• New hazards found?

Outputs and Measures
Does the organization use the Safety Risk Management (Component 2.0) if risk assessment and risk control performance indicates -
• That new hazards or potential hazards have been found?
• That the system needs to be changed?
Does the organization maintain records of assessments in accordance with the requirements of SMS Documentation and Records Element 1.5?
Does the organization identify interfaces between the system assessment function and -
• The hazard identification function (2.1.2, Identify Hazards Element)?
• The preventive and corrective action function (3.3.1, Preventive/Corrective Action Element)?
Does the organization periodically measure performance objectives and design expectations of the System Assessment Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the System Assessment Process?

Bottom Line Assessment:

Has the organization assessed risk controls' performance and effectiveness, conformance with SMS requirements, and the objectives of the Safety Policy?

Element 3.2 - Management of Change

Performance Objective:

The organization's management will identify and determine acceptable safety risk for changes within the organization that may affect established processes and services by new system design, changes to existing system designs, new operations/procedures, or modified operations/procedures.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from proposed changes to systems, processes, procedures, or organizational structures?
Management Responsibility
Does the organization will clearly identify who is responsible for the quality of the Management of Change Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization ensure it does not implement any of the following until the level of safety risk of each identified hazard is determined to be acceptable for -
• New system designs?
• Changes to existing system designs?
• New operations or procedures?
• Modifications to existing operations or procedures?
Outputs and Measures
Does the organization: • Ensure that this process is interfaced with the SRM process (System Description and Task Analysis 2.1.1)? and • Periodically measure performance objectives and design expectations of the Management of Change Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Management of Change Process.

Bottom Line Assessment:

Has the organization's management assessed risk for changes within the organization that may affect established processes and services by new system designs, changes to existing system designs, new operations/procedures or modified operations/procedures?

Element 3.3 Continuous Improvement

Performance Objective:

The organization will promote continuous improvement of its SMS through recurring application of SRM (Component 2.0), SA (Component 3.0), and by using safety lessons learned and communicating them to all personnel.

Design Expectations
Input
Are inputs (interfaces) for this process obtained through continuous application of Safety Risk Management (Component 2.0), Safety Assurance (Component 3.0) and the outputs of the SMS, including safety lessons learned?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Continual Improvement Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization continuously improve the effectiveness of the SMS and of safety risk controls through the use of the safety and quality policies, objectives, audit and evaluation results, analysis of data, corrective and preventive actions, and management reviews?
Does the organization develop safety lessons learned? and -
• Use safety lessons learned to promote continuous improvement of safety?
• Ensure that safety lessons learned are communicated to all personnel?
Outputs and Measures
Does the organization: • Ensure that trend analysis of safety and quality policies, objectives, audit and evaluation results, analysis of data, and corrective and preventive actions are interfaced with Management Review Process 3.3.2, below?, and • Periodically measure performance objectives and design expectations of the Continual Improvement Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Continuous Improvement Process?

Bottom Line Assessment:

Has the organization promoted continuous improvement of its SMS through recurring application of Safety Risk Management (Component 2.0), Safety Assurance (Component 3.0), and by using safety lessons learned and communicating them to all personnel?

Element 3.3 Continuous Improvement

Process 3.3.1 Preventive/Corrective Action

Performance Objective:

The organization will take preventive and corrective action to eliminate the causes or potential causes of nonconformance identified during analysis, to prevent recurrence.

NOTE: Although Process 2.2.3 (Control/Mitigate Safety Risk) is very similar to Process 3.3.1, the primary differences are:

- Process 2.2.3 is used during the design of a system (often looking to the future) or in the redesign of a non-performing system where system requirements are being met, but the system is not producing the desired results.

- Process 2.2.3 is also used where new hazards are discovered during Safety Assurance that was not taken into account during initial design.

- Process 3.3.1 is used to develop actions to bring a non-performing system back into conformance to its design requirements.

Design Expectations
Inputs
Are inputs (interfaces) for this process obtained from System Assessments (Process 3.1.8) with findings of non-performing risk controls?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Preventive/Corrective Action Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization develop the following -
• Preventive actions for identified potential nonconformities with risk controls?
• Corrective actions for identified nonconformities with risk controls?
Does the organization consider safety lessons learned in the development of -
• Preventive actions?
• Corrective actions?
Does the organization take necessary preventive and corrective action based on the findings of investigations?
Does the organization prioritize and implement preventive and corrective actions in a timely manner?

Outputs and Measures
Does the organization keep and maintain records of the disposition and status of preventive and corrective actions according to established record retention policy?
Does the organization: • Identify interfaces between this process and the Continuous Monitoring Process 3.1.1 above? and • Periodically measure performance objectives and design expectations of the Preventive and Corrective Action Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Preventive and Corrective Action Process?

Bottom Line Assessment:

Has the organization taken preventive or corrective actions to eliminate the causes of non-conformances, identified during analysis, to prevent recurrence?

Element 3.3 Continuous Improvement

Process 3.3.2 - Management Review

Performance Objective:

Top management will conduct regular reviews of the SMS to assess the performance and effectiveness of an organization’s operational processes and the need improvements.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the outputs of Safety Risk Management (Component 2.0) and Safety Assurance (Component 3.0) activities including – • Hazard identification (Process 2.1.2)? • Risk analysis (severity and likelihood) (Process 2.2.1)? • Risk assessments (Process 2.2.2)? • Risk control/mitigation plans (Process 2.2.3)? • Results of analysis of data (Process 3.1.7)?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Management Review Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does top management conduct regular reviews of the SMS, including the outputs of the Safety Risk Management Processes, the outputs of the Safety Assurance Processes, and safety lessons learned?
Does top management include in its reviews of the SMS, an assessment of the need for improvements to the organization's operational processes and the SMS?
Outputs and Measures
Does the organization keep records of the disposition and status of management reviews according to the organization's record retention policy?
Does the organization: • Identify interfaces between this process and the Hazard Identification Process (2.1.2, above) and Preventive and Corrective Action Process (3.3.1, above)? and • Periodically measure performance objectives and design expectations of the Management Review Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Management Review Process?

Bottom Line Assessment:

Has top management conducted regular reviews of the SMS, including outputs of Safety Risk Management (Component 2.0), Safety Assurance (Component 3.0), and lessons learned? Has management reviews included assessing the performance and effectiveness of an organization's operational processes and the need for improvements?

Component 4.0 - Safety Promotion

Component Performance Objective:

Top management will promote the growth of a positive safety culture and communicate it throughout the organization.

Component Design Expectations
Input
Are inputs (interfaces) identified between top management and organizational personnel?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Safety Promotion Component (4.0)? Do procedures will also define who is responsible for accomplishing the process?
Procedure/Output/Measure
Does top management promote the growth of a positive safety culture through -
• Publication of top management's stated commitment to safety to all employees?
• Visible demonstration of their commitment to the SMS?
• Communication of the safety responsibilities for the organization's personnel?
• Clear and regular communication of safety policy, goals, expectations, standards, and performance to all employees of the organization?
• An effective employee reporting and feedback system that is non-punitive and provides confidentiality?
• Use of a safety information system that provides an accessible efficient means to retrieve information?
• Allocation of resources essential to implement and maintain the SMS?
Does the organization will periodically measure performance objectives and design expectations of the Safety Promotion Component?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the Safety Promotion Component?

Bottom Line Assessment:

Has top management promoted the growth of a positive safety culture and communicate it throughout the organization?

Element 4.1 Competencies and Training

Process 4.1.1 - Personnel Expectations (Competence)

Performance Objective:

The organization will document competency requirements for those positions identified in Element 1.2 and 1.3 and ensure those requirements are met.

Design Expectations
Input
Are inputs (interfaces) for this process identified between top management and the key safety personnel referenced in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Personnel Expectations Process? Do procedures will also define who is responsible for accomplishing the process?
Procedure
Does the organization identify the competency requirements for safety-related positions identified in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3?
Outputs and Measures
Does the organization ensure that the personnel in the safety-related positions identified in Management Commitment and Safety Accountabilities Element 1.2 & Key Safety Personnel Element 1.3 meet the documented competency requirements of Personnel Expectations Process 4.1.1?
Does the organization periodically measure performance objectives and design expectations of the Personnel Expectations Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the personnel qualification and training process?

Bottom Line Assessment:

Has the organization documented competency requirements for those positions identified in Management Commitment and Safety Accountabilities Element 1.2 and Key Safety Personnel Element 1.3 and ensured those requirements were met?

Element 4.1 Competencies and Training

Process 4.1.2 - Training

Performance Objective:

The organization will develop, document, deliver and regularly evaluate training necessary to meet competency requirements of Process 4.1.1.

Design Expectations
Input
Are inputs (interfaces) for the Training Process obtained through the outputs of the SMS and the documented competency expectations of Personnel Expectations Process 4.1.1?
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the SMS Training Process? Do procedures define who is responsible for accomplishing the process?
Procedure
Does the organization's training meet the competency expectations of Personnel Expectations Process 4.1.1 for the personnel in the safety-related positions identified in Management Commitment and Safety Accountability Element 1.2 & Key Safety Personnel Element 1.3?
Does the organization consider scope, content, and frequency of training required to meet and maintain competency for those individuals in the positions identified in Management Commitment and Safety Accountability Element 1.2 and Key Safety Personnel 1.3?
Does the organization's employees receive training commensurate with their -
• Position level within the organization?
• Impact on the safety of the organization's products or services?
Does the organization maintain training currency by periodically -
• Reviewing the training?
• Updating the training?

Outputs and Measures
Does the organization maintain records of required and delivered training?
Does the organization: • Identify interfaces between safety lessons learned and the training functions, as well as the interfaces between the training functions and the delivery of training deemed to be necessary to meet competency requirements of (4.1.1, above), and • Periodically measure performance objectives and design expectations of the SMS Training Process.
Controls
Does the organization ensure that safety-related training media is periodically reviewed and updated for target populations?
Does the organization ensure that: • Procedures are followed for safety-related operations and activities? and • They periodically review supervisory and operational controls to ensure the effectiveness of the SMS Training Process?

Bottom Line Assessment:

Has the organization developed, documented, delivered and regularly evaluated training necessary to meet competency expectations of the Personnel Expectations Process 4.1.1?

Element 4.2 - Communication and Awareness

Performance Objective:

Top management will communicate the output of its SMS to its employees, and will provide its oversight organization access to SMS outputs in accordance with established agreements and disclosure programs.

Design Expectations
Input
Are inputs (interfaces) for this process obtained from the outputs of Safety Risk Management (2.0) and Safety Assurance (3.0) Components, including- • Hazard identification? (2.1.2) • Risk severity and likelihood? (2.2.1) • Risk assessments? (2.2.2) • Risk control/mitigation plans? (2.2.3) • Safety lessons learned? • Results of analysis of data? (3.1.7)
Management Responsibility
Does the organization clearly identify who is responsible for the quality of the Communication and Awareness Process? Do procedures define who is responsible for accomplishing the process?
Procedure/Output/Measure
Does the organization ensure it communicates outputs of the SMS, rationale behind controls, preventive and corrective actions and ensures awareness of SMS objectives to its employees?
Does the organization ensure it provides its oversight organization access to the outputs of the SMS in accordance with established agreements and disclosure programs?
Does the organization interface with other organization's SMSs to cooperatively manage issues of mutual concern?
Does the organization will periodically measure performance objectives and design expectations of the Communication and Awareness Process?
Controls
Does the organization ensure that: • Procedures are followed for safety-related operations and activities?, and • They periodically review supervisory and operational controls to ensure the effectiveness of the Communication and Awareness Process?

Bottom Line Assessment:

Has top management communicated the output of its SMS to employees and provided its oversight organization access to SMS outputs in accordance with established agreements and disclosure programs?

APPENDIX D - SAFETY RISK MANAGEMENT (SRM)

(PROCESSES AND TOOLS)

D.1 INTRODUCTION.

This appendix describes fundamental Safety Risk Management (SRM) concepts, discusses what types of changes are evaluated for safety risk, and details the process and guidance available for determining if a change requires a complete safety analysis under SRM. SRM (SMS Component 2.0) is one of the two core operational activities under an SMS (the other being SMS Component 3.0 – Safety Assurance). The management of change (SMS Element 3.2) is also directly related to this subject. This chapter is being provided to supplement guidance on Component 2.0 – SRM and Element 3.2 – Management of Change that is contained in Chapters 2 and Chapter 4 concerning Safety Risk Management (SRM). The chapter also outlines the process of assessing and managing safety risk, including:

- Definitions of commonly used terms
- Descriptions of safety analysis activities early in the planning or change proposal process
- Descriptions of the evidence and documentation that indicate that the objectives have been met

NOTE: The exact processes and methodologies described in this appendix are not mandatory (e.g. use of SRM Panels, need for Safety Engineers, etc.) and need not necessarily be followed by all aviation organizations when managing every change. Processes and methodologies must be tailored to meet the specific characteristics and needs of individual aviation organizations. In all cases however, the aviation organization’s Safety Risk Management functions must conform to the SMS framework.

This document describes the documentation necessary for safety analyses and the required components of the documentation. In addition, it provides information on how organizations should formally document (and approve) their SRM activities and outputs, accept risk and track changes.

NOTE: See Figure 9 at the end of this appendix for a glossary of terms used throughout this appendix

D.2 SRM OVERVIEW.

Changes to any system create the potential for increased safety risk as the changes interact or interface with existing procedures, systems, or operational environments. Aviation personnel can use SRM to maintain or improve safety by identifying, managing, and mitigating the safety risk associated with all changes (e.g., changes to systems (hardware and software), equipment, and procedures) that impact safety.

a) *SRM DEFINED.* SRM is a formalized, proactive approach to system safety. SRM is a methodology applied to all changes that ensures hazards are identified, and unacceptable risk is mitigated and accepted prior to the change being made. In this context, a change could be any change to or modification of airspace; aerodromes; aircraft; maintenance programs; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components. It provides a framework to ensure that once a change is made, it continues to be tracked throughout its lifecycle.

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

ii. The SRM process is a means to:

• Document proposed changes regardless of their anticipated safety impact

• Identify hazards associated with a proposed change

• Assess and analyze the safety risk of identified hazards

• Mitigate unacceptable safety risk and reduce the identified risks to the lowest possible level

• Accept residual risks prior to change implementation

• Implement the change and track hazards to resolution

• Assess and monitor the effectiveness of the risk mitigation strategies throughout

the lifecycle of the change

• Reassess change based on the effectiveness of the mitigations

b) *SYSTEM, HAZARD and RISK DEFINED.* Three important terms necessary to discuss making changes to aviation-related systems, the resulting potential hazards, and the management of risk are:

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

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

iii. Risk. Risk is the product of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. Severity, likelihood, and system state will be defined later in this document.

NOTE: The system safety methodology, as described in this section, addresses risk on an individual hazard-by-hazard basis and, therefore, does not address aggregate safety risk. Aviation personnel can determine risk acceptability using the risk matrix in Figure 8.

c) *DEFENSES IN DEPTH - DESIGNING AN ERROR TOLERANT SYSTEM.* Given the complex interplay of human, material, and environmental factors in operations, the complete elimination of risk is an unachievable goal. Even in organizations with the best training programs and a positive safety culture, human operators will occasionally make errors; the best-designed and maintained equipment will occasionally fail. System designers take these factors into account and strive to design and implement systems that will not result in an accident due to an error or equipment failure. These systems are referred to as “error tolerant.”

i. Error Tolerant System. An error tolerant system is defined as a system 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.

ii. Developing a Safe and Error Tolerant System. The system is required to contain multiple defenses allowing no single failure or error to result in an accident. An error tolerant system includes mechanisms that will recognize a failure or error, so that corrective action will be taken before a sequence of events leading to an accident can develop. The need for a series of defenses rather than a single defensive layer arises from the possibility that the defenses may not always operate as designed. This design philosophy is called “defenses in depth.”

iii. Failures in the Defensive Layers. An operational system can create gaps in the defenses. As the operational situation or equipment serviceability states change, gaps may occur as a result of:

1. Undiscovered and longstanding shortcomings in the defenses

2. The temporary unavailability of some elements of the system as the result of maintenance action

3. Equipment failure

4. Human error or violation

iv. Design Attributes. Design attributes of an error tolerant system include:

1. Making errors conspicuous (error evident systems)

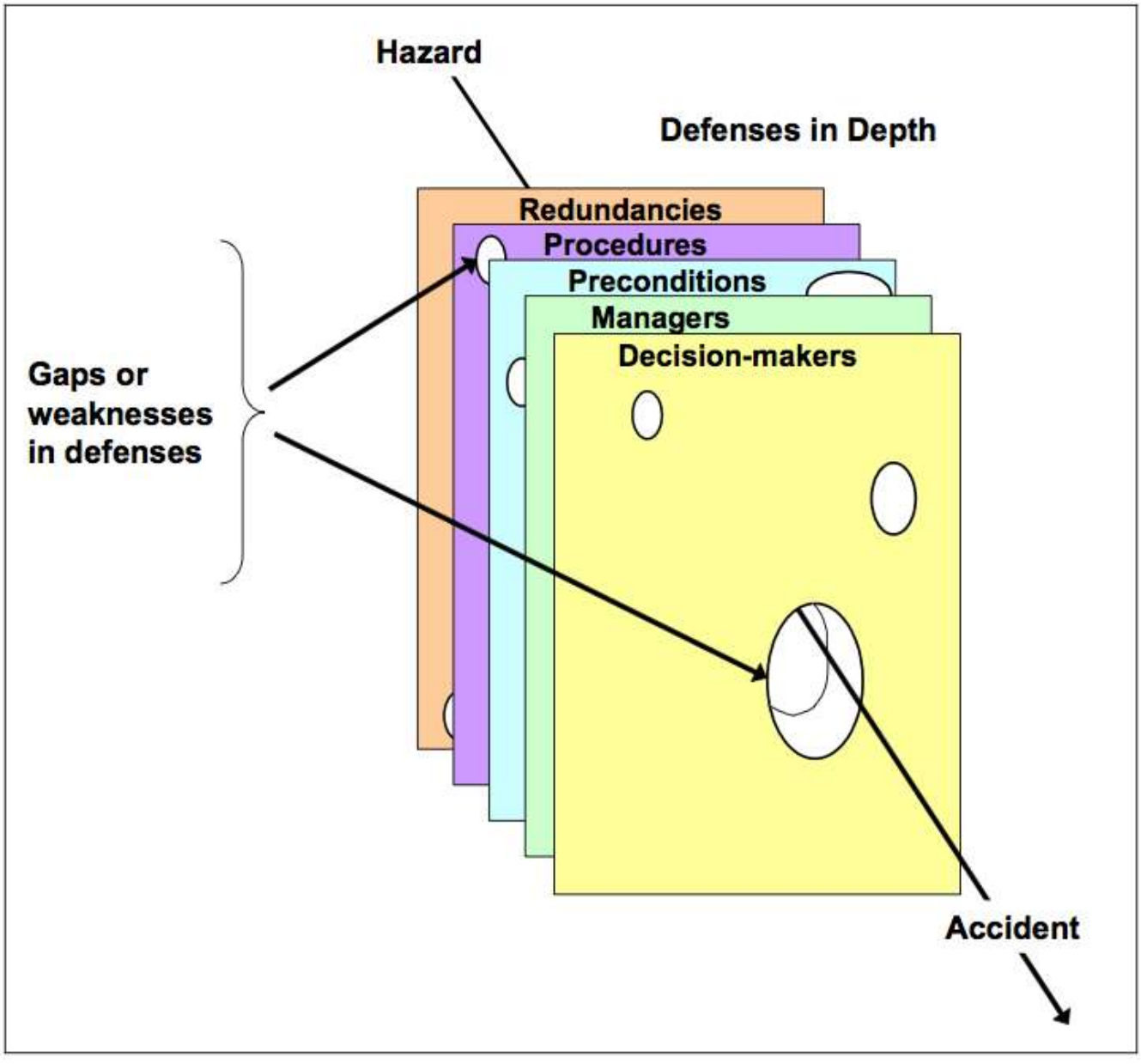
2. Trapping the error to prevent it from affecting the system (error captive systems)

3. Detecting errors and providing warning and alerting systems (error alert systems)

4. Ensuring that there is a recovery path (error recovery systems)

v. Well-Designed System. For an accident to occur in a well-designed system, these gaps must develop in all of the defensive layers of the system at the critical time when that defense should have been capable of detecting the earlier error or failure. An illustration of how an accident event must penetrate all defensive layers is shown in Figure 1. This concept is commonly referred to as James Reason’s “Swiss Cheese” model.

Figure 1. Defenses in Depth Philosophy



vi. Gaps in System Defenses. The gaps in the system's defenses shown in Figure 1. are not necessarily static. Gaps "open" and "close" as the operational situation, environment, or equipment serviceability states change. A gap may sometimes be the result of nothing more than a momentary oversight on the part of a controller or operator. Other gaps may represent long-standing latent failures in the system.

vii. Latent Failure. A latent failure is considered a failure that is not inherently revealed at the time it occurs. For example, in an electrically powered system, when there is a slowly degrading back-up battery that has no state-of-charge sensor, the latent failure would not be identified until the primary power source failed and the back-up battery was needed. If no maintenance procedures exist to periodically check the battery, the failure would be considered an undetected latent event.

d) *DETECTING GAPS.* The task of reducing risk can be applied in both proactive and reactive ways. Careful analysis of a system and operational data monitoring make it possible to identify sequences of events where faults and errors (either alone or in combination) could lead to an incident or accident before it actually occurs. The same approach to analyze the chain of events that lead to an accident can also be used after the accident occurs. Identifying the active and latent failures revealed by this type of analysis enables one to take corrective action to strengthen the system's defenses.

e) *CLOSING GAPS.* The following examples of typical defenses used in combination to close gaps are illustrative and by no means a comprehensive list of solutions:

i. Equipment:

• Redundancy

o Full redundancy providing the same level of functionality when operating on the alternate system

o Partial redundancy resulting in some reduction in functionality (e.g., local copy of essential data from a centralized network database)

• Independent checking of design and assumptions

• System designed to ensure that a critical functionality is maintained in a degraded mode in the event that individual elements fail

• Policies and procedures regarding maintenance, which may result in loss of some functionality in the active system or loss of redundancy

• Automated aids or diagnostic processes designed to detect system failures or processing errors and report those failures appropriately

- Scheduled maintenance

ii. Operating Procedures:

- Adherence to standard terminology/phraseology and procedures
- Confirmation of critical items in instructions
- Checklists and habitual actions
- Training, analyses, and reporting methods

iii. Organizational Factors:

- Management commitment to safety
- Current state of safety culture
- Clear safety policy
    - o Implemented with adequate funding provided for safety management activities
- Oversight to ensure correct procedures are followed
    - o No tolerance for willful violations or shortcuts
- Adequate control over the activities of contracted personnel outside the organization

f) *EFFECT OF HARDWARE AND SOFTWARE ON SAFETY.* System designers generally design the hardware and software components of a system to meet specified levels of reliability, maintainability, and availability. The techniques for estimating system performance in terms of these parameters are well established. When necessary, system designers can build redundancy into a system, to provide alternatives in the event of a failure of one or more elements of the system.

i. Designers use system redundancy and hardware and/or software diversity to provide service in the event of primary system failures. Different hardware and software meet the functional requirements for the back-up mode.

ii. Physical diversity is another method system designers use to increase the likelihood of service availability in the event of failures. Physical diversity involves separating redundant functions so that a single point of failure does not corrupt both paths, making the service unavailable. An example of physical diversity would be to bring an electrical power supply into a system through two different locations. In the event of a fire or other issue in one location, the alternate path would still provide power, which increases the likelihood that the system would remain available.

iii. When a system includes software and/or hardware, the safety analyses consider possible design errors and the hazards they may create. Systematic design processes are an integral part of detecting and eliminating design errors.

g) *HUMAN ELEMENT'S EFFECT ON SAFETY*. Ultimately, every system exists to assist a human in task performance. Therefore, system designers must design the human-to-the-system interface and associated procedures to capitalize on human capabilities and to compensate for human limitations. One limitation is human performance variability, which necessitates careful and complete analysis of the potential impact of human error. Machines and systems are built to function within specific tolerances, so that identical machines have identical, or nearly identical, characteristics. By contrast, humans vary due to genetic and environmentally determined differences. Designers take these differences into account when designing products, tools, machines, and systems to "fit" the target user population. Human capabilities and attributes differ in areas such as:

- Sense modalities (manner and ability of the senses, such as seeing, hearing, and touching)
- Cognitive functioning
- Reaction time
- Physical size and shape
- Physical strength

i. Fatigue, illness, and other factors such as stressors in the environment, noise, and task interruption also impact human performance. Designers use Human Error Analysis (HEA) to identify the human actions in a system that can create hazardous conditions. Optimally, the system is designed to resist human error (error resistant system) or at a

minimum, to tolerate human error (error tolerant system).

ii. Human error is estimated to have been a causal factor in 60 to 80 percent of aviation accidents and incidents and is directly linked with system safety, error, and risk. People make errors, which have the potential to create hazards. In addition, accidents and incidents often result from a chain of independent errors. For this reason, system designers must design safety-critical systems to eliminate as many errors as possible, minimize the effects of errors that cannot be eliminated, and lessen the negative impact of any remaining potential human errors.

iii. As a general rule, “human factors” can be defined as 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, effective human performance.”

iv. Human factors is a discipline that examines the human role in a system or application (e.g., hardware, software, procedure, facility, document, other entity) and how the human is integrated into the design. Human factors applies knowledge of how humans function in terms of perception, cognition, and biomechanics to the design of tools, products, and systems that are conducive to human task performance and protective of human health and safety.

v. When examining adverse events attributed to human error, often elements of the human-to-system interface (such as display design, controls, training, workload, or manuals and documentation) are flawed. Human reliability analysis and the application of human performance knowledge must be an integral part of the SMS; affecting system design for safety-critical systems. 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 human-centered design approach is central to the concept of managing human errors that affect safety risk.

D.3 APPLICABILITY OF SRM TO MANAGEMENT OF CHANGE.

All proposed changes (e.g., new equipment; systems; modifications to existing equipment, systems and new and/or changes to existing procedures; operations; and policies) should trigger an SRM evaluation. Figure 2 below provides an overview of SRM and its steps.

Figure 2. SRM Steps

D.4 PLANNING.

a) Planning the SRM effort requires that an individual:

• Decides the level and type of safety analysis that is needed

• Coordinates with other organizations that may be affected by the change or the risk mitigation strategies

b) The scope of the SRM effort is a function of the nature, complexity, and impact or consequence of the change. It is critical that the scope and complexity of the safety analysis match the scope and complexity of the change. To support this activity in larger organizations, the originating department should consult an expert in system safety to determine if additional involvement from other organizations is needed.

c) It is important for the group designated as an “SRM Panel” to recognize how systems or items initially determined to have no impact on safety could potentially impact the system or change being analyzed. For instance, air conditioning may not initially appear to have an impact on the safety of a larger system; however, when that system depends on air conditioning to keep it from overheating and failing, air conditioning (or lack thereof) could impact the safety of that system, as well as the safety of the operation as a whole. Issues or potential hazards captured through the SRM process/analysis, but not directly the result of the change being assessed, must be formally passed or transferred onto the appropriate party, and appropriately documented.

d) SRM Panel. An SRM Panel should include representatives and stakeholders from the various organizations affected by the change. It is important that the panel be made up of an appropriately diverse team, including stakeholders and experts, who will be involved, in different capacities, throughout the safety analysis process. A “stakeholder” is a group or individual that is affected by, or is in some way accountable for the outcome of, an 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.

i Though the size and make-up of the panel will vary with the type and complexity of the proposed change, involving the following types of expertise on the SRM Panel should be considered (list not all-inclusive):

- Employees directly responsible for developing the proposed change
- Employees with current knowledge of and experience with the system or change
- Hardware and/or software engineering or automation expert to provide knowledge on equipment performance
- SRM specialist to guide the application of the methodology
- Human factors specialist
- Software specialist
- Systems specialist
- Employees skilled in collecting and analyzing hazard and error data and using specialized tools and techniques (e.g., operations research, data, human factors, failure mode analysis)

e) Panel Facilitator Responsibilities. For each SRM Panel, there should be one person who serves as the SRM Panel facilitator. The facilitator or a member of the SRM Panel collects information relevant to the change. This information may include meeting with the person who proposed the change. The change proponent must clarify the:

- Current system state or condition
- Proposed change
- Intent of the change
- System state(s) in which the change will be conducted
- Boundaries of the analysis

• Assumptions that may influence the analysis

i The SRM Panel facilitator ensures that the following occurs:

• Potential panel members are identified

• Panel members have a common understanding of the SMS and SRM principles

• Material required for the first meeting is gathered, including:

o Preliminary Hazard Lists (PHLs) of similar changes

o Collection and analysis of data appropriate to the change to assist in hazard identification and risk assessment

o SRM handouts (severity and likelihood table and risk matrix, as shown in Figure 8.

• Panel members are aware of meeting logistics

• Co-facilitator is identified (co-facilitator will later work with the facilitator and the change proponent to help prepare the final safety document)

• SRM Panel orientation is prepared (i.e. why we are here, what are we trying to accomplish, what is our schedule, etc.)

• Initial set of SRM Panel ground rules are developed (i.e. how the panel members will interact with each other)

ii At the initial meeting, the facilitator must present a panel orientation, including:

• Summary of the goals and objectives for the panel

• Brief review of the SRM process

• Development of SRM Panel ground rules

• Determination of how often the SRM Panel will meet along with location, time, and date

• Presentation of the proposed change with the sample PHL data and other information pertinent to the change

iii Involving panel members with varying experience and knowledge leads to a broader, more comprehensive, and more balanced consideration of safety issues than an individual assessment. The following is a recommended process for the SRM Panel:

• Individuals use the group session to generate ideas and undertake preliminary assessment only (perhaps identifying factors that are important, rather than working through the implications in detail)

• A subset of the panel with sufficient breadth of expertise to understand all the issues raised and a good appreciation of the purposes of the assessment, collate and analyze the findings after the session. The person who facilitated or recorded the session often is most able to perform this task

• The individuals who collate and analyze the results present them to the group to check that input has been correctly interpreted. This also gives the group a chance to reconsider any aspect once they can see the whole picture

D.5 PRELIMINARY SAFETY ANALYSIS.

a) Required Levels of Safety Analysis. When proposing a change to a system, change proponents must perform a preliminary safety analysis. If the change does not affect the overall system, there is no need to conduct a further safety analysis. If the change does affect the system, a fundamental question to ask is: does the change have the potential to introduce safety risk into the overall system? Figure 3 describes the process for determining what type of safety analysis is required under SRM. Additional questions to make that determination may include:

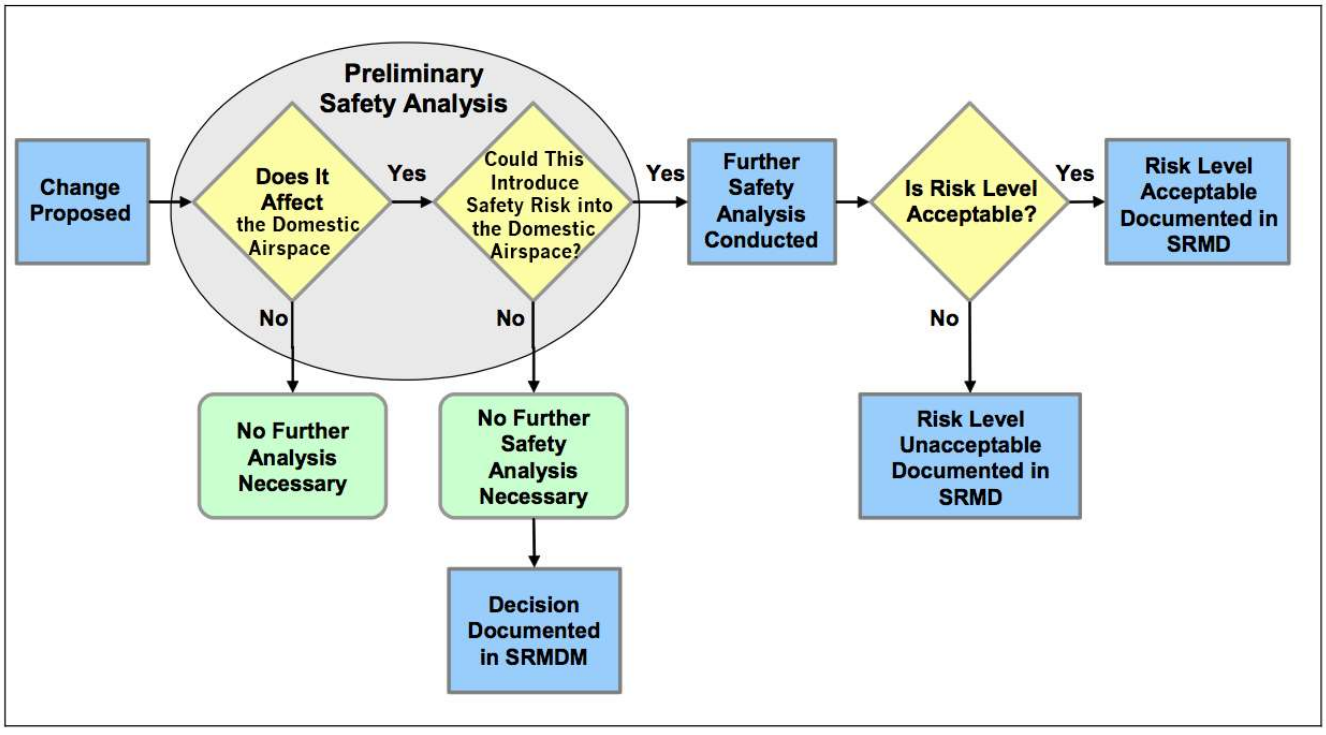
• Does the change affect certificate holder and GACA interaction?

• Does the change affect existing processes or procedures?

• Does the change represent a change in operations?

• Does the change modify the form, fit, and/or function of a critical system?

Figure 3. SRM Decision Process



i If the change is not expected to introduce safety risk, then there is no need to conduct further safety analysis; instead, the change proponent documents that determination, along with the justification for the decision as to why the change is not subject to the provisions of additional SRM assessments and supporting documentation beyond the initial safety analysis in an SRM Decision Memo (SRMDM), described in Section 9 B. If the change is expected to impact safety, it is necessary to conduct further safety analysis and document the safety analysis in a Safety Risk Management Document (SRMD). Even when a change is proposed to improve safety, the need to conduct further safety analysis remains.

ii The level at which an organization conducts SRM varies by organization, change proponent, and/or type of change. Not all changes affect or require further safety analysis.

b) SRMDM: No Safety Risk Introduced to the Civil Aviation Environment. In the early stages of analysis, it may become evident that a change does not introduce any safety risk into the civil aviation environment or for a certificate holder. In this case, there is no need to further assess the safety risk. The SRMDM can be used to document all proposed changes that do NOT introduce any safety risk (hazards) to the civil aviation environment or for a certificate holder's operations. Such determinations can be made by the change proponent, affected departments, or

an SRM Panel. The SRMDM must include a description of the proposed change and the justification for the decision that the change is not subject to the provisions of additional SRM assessments, and supporting documentation beyond the preliminary safety analysis. The justification must describe the rationale supporting the finding that the proposed change does NOT introduce any safety risk to the civil aviation environment or a certificate holder's operations. All SRM documentation, including SRMDMs, must be kept on file throughout the lifecycle of a system or change.

i It is recommended that an SRMDM have two signatures at a minimum, one from the change proponent and one from a designated management official of the affected aviation organization. Such organizations may have additional signatory requirements as well.

D.6 WHEN FURTHER SAFETY ANALYSIS IS REQUIRED.

a) SRM Safety Analysis Phases. Consistent with ICAO guidelines and best practices, the SRM phases in Figure 4 are equally applicable to any SRM activity, whether it pertains to operations, maintenance, procedures, or new system development. Figure 5 illustrates how the five phases of the SRM safety analysis are accomplished. Systematically completing these steps creates a thorough and consistent safety analysis.

Figure 4. SRM Safety Analysis Phases

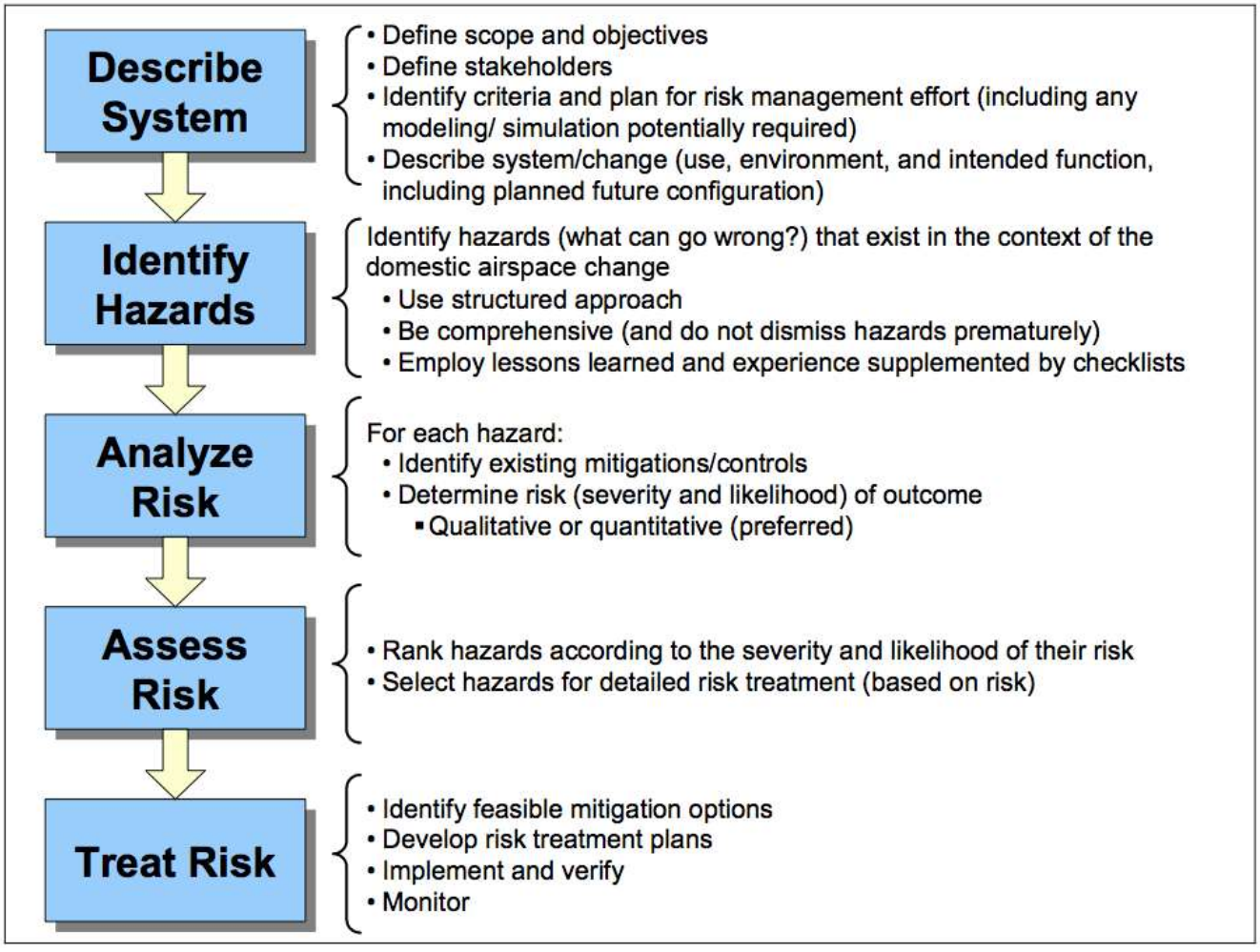
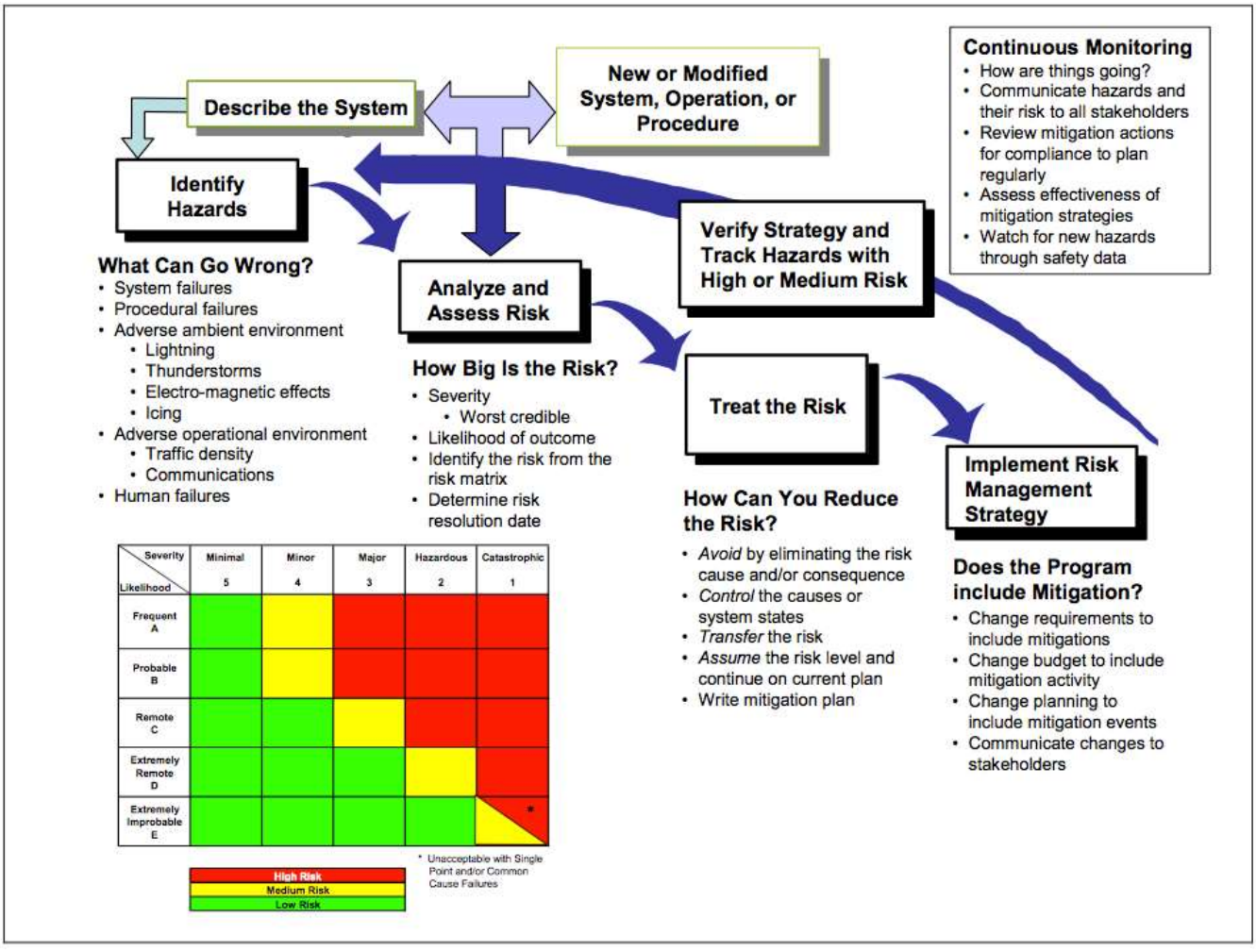


Figure 5. How to Accomplish a Safety Analysis



b) The safety steps are closed-loop, meaning those tasked with executing SRM repeat one or more steps until the safety risk for each hazard is acceptable. Regardless of the phase of operation, these steps assist SRM practitioners in identifying and managing the safety risk associated with providing particular civil aviation services.

D.7 PHASE 1: DESCRIBE SYSTEM.

a) Describing the System. A good system description is the critical foundation for conducting a sound safety analysis. The system description provides information that serves as the basis to identify all hazards and associated safety risks. It is critical that the SRM Panel members:

b) Define and document the scope and objectives of the proposed change or system.

c) Describe and model the system and operation in sufficient detail for the safety analysis to proceed to the next stage—identifying hazards (e.g., modeling might entail creating a functional flow diagram to help depict the system and the interface with the users, other systems, or sub-systems).

d) Are aware that the system is always a sub-component of some larger system. For example, even if the analysis encompasses all services provided within an entire area, it can be considered a subset of a larger area, which in turn, is a subset of a larger part of the system.

e) Potential Effects on the System or Interfacing Systems. This phase considers all critical factors. The resulting description defines the scope of the risk assessment. A complete and accurate system description is the essential foundation for conducting a thorough safety analysis. System descriptions need to exhibit two essential characteristics—correctness and completeness.

- Correctness in a description means that it 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

f) A description of the change may be a full report or a paragraph; length is not important, as long as the description covers all of the essential elements. It is vital that the description of the proposed change be correct and complete. If the description is too vague, incomplete, or otherwise unclear, it must be clarified before continuing the safety analysis. Questions to consider include:

- What is the purpose of the system or change?
- How will the system or change be used?
- What are the system or change functions?
- What are the system or change boundaries and external interfaces?
- What is the environment in which the system or change will operate?
- What are the interconnectivity and/or interdependencies between systems?

• How will the change impact system users?

g) The following are examples of data that the people conducting the safety analysis could consider when describing the system:

• Average volume of work products

• Number of hours worked or flown

• Number and type of operations

• Number of aircraft controlled

• Number of VFR vs. IFR hours flown

• Availability and reliability for both hardware and software

• Number of errors, violations, or deviations

• Number of accidents or incidents

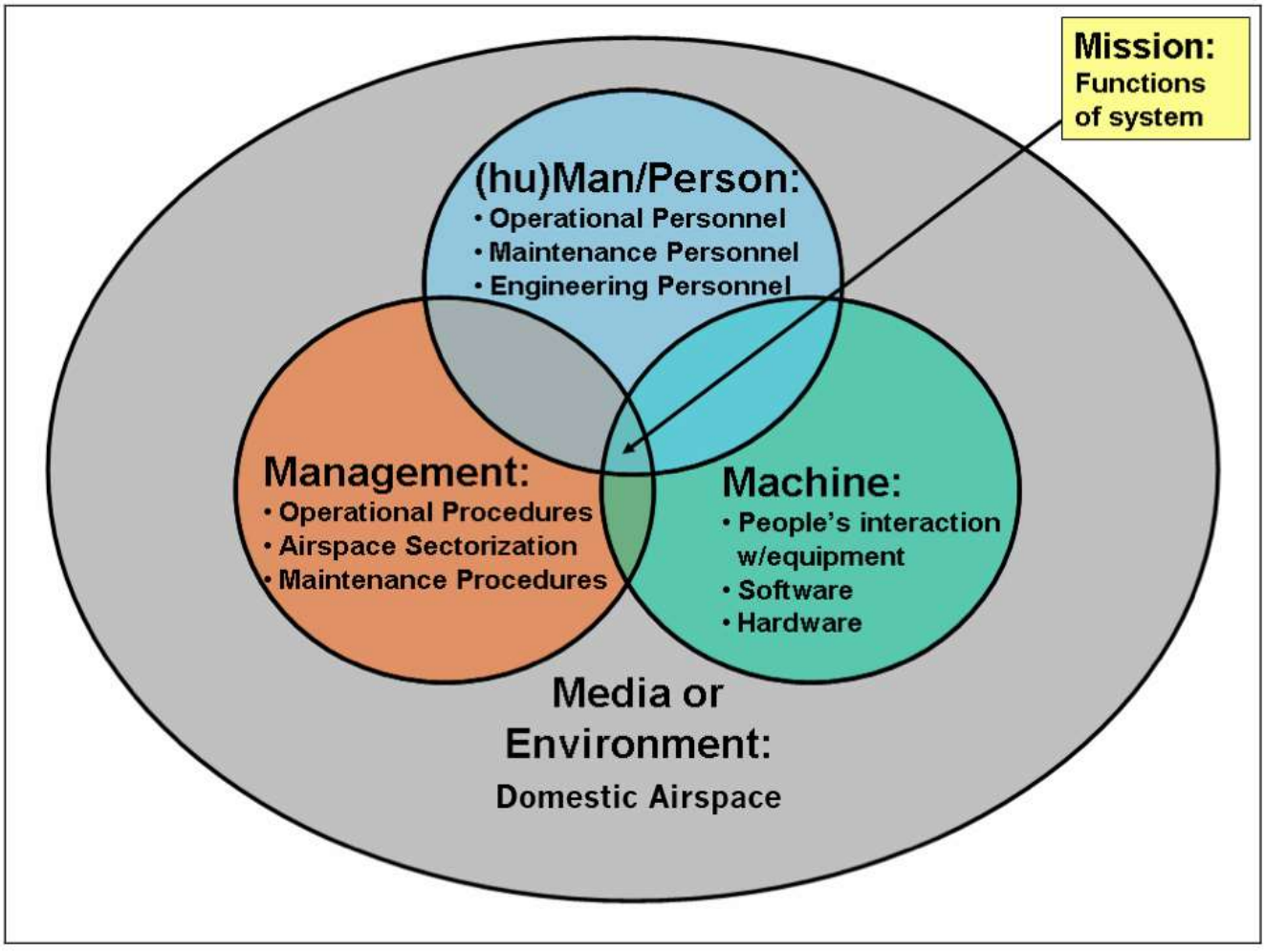
• Number of worker injuries

• Accident/injury data

NOTE: The Safety Assurance of an SMS can be used to provide potential sources of data to be used in an SRM.

h) 5M Model of System Description. SRM Panels can use a variety of methods to create a system description. The 5M Model shown in Figure 6 is one useful method to capture the information needed to describe the system.

Figure 6. 5M Model



i) The 5M Model illustrates five integrated elements in any system:

• Mission. The functions that the system needs to perform

• Man/Person. The human operators and maintainers

• Machine. The equipment used in the system including hardware, firmware, software, human-to-system interface, and avionics

• Management. The procedures and policies that govern the system's behavior

• Media. The environment in which the system is operated and maintained

j) The 5M Model and similar techniques are used to deconstruct the proposed change to

distinguish elements that are part of, or impacted by, the proposed change. These elements will later help to identify sources, causes, hazards, as well as current (and proposed) hazard mitigations.

k) Bounding the System: Limit Analysis to Scope of the Change. Bounding means limiting the analysis of the change or system to the elements that affect or interact with each other to accomplish the central function. The level of detail in the description varies, typically proportionally to the breadth of the change. The system description has both breadth and depth. Breadth refers to the system boundaries, and depth refers to the level of detail in the description. A thorough system description and the elements within it constitute the potential sources of hazards associated with the proposed change. This is critical to the subsequent phases of the SRM process.

l) The resulting bounded system description limits the analysis to the components necessary to adequately assess the safety risk associated with the change.

m) Required Depth and Breadth of the Analysis. The depth and breadth of the analysis necessary for SRM varies. Some of the factors used to determine the depth and breadth of the analysis include:

• The Size and Complexity of the Change Under Consideration. A larger and more complex change may also require a larger and more complex analysis.

• The Breadth of a Change. SRM scope can be expected to increase if the change spans more than one organization, or department within an organization.

• The Type of Change. Procedural- or equipment-driven changes tend to require more analysis than a frequency change.

i. Selecting the appropriate scope and detail of the safety analysis is critical. The SRM Panel takes multiple factors into consideration when making these determinations. In general, safety analyses on more complex and far-reaching changes will require a greater scope and detail. For example, a major acquisition program could require multiple safety analyses involving hundreds of pages of data at the preliminary, sub-system, and system levels, evaluating numerous interfaces with other systems, operators, and maintainers. However, an operational procedure change at a lower level within a particular organization may require a less intensive analysis that describes the change and identifies the hazards

and associated risks. In both cases, the SRM requirements are met, but the safety analysis is tailored to meet the needs of the decision-makers. “A primary consideration in determining what both the scope and detail of the safety analysis are”. In other words, what information is required to know enough about the change, the associated hazards, and each hazard’s associated risk to choose which controls to implement and whether to accept the risk of the change. The scope of the analysis enables the making of informed decisions about whether the proposed change is acceptable for implementation from a safety perspective. If there is doubt about whether to include a specific element in the analysis, it is better if the panel includes that item at first, even though it might prove irrelevant during the hazard identification phase.

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

1. Sufficient understanding of system boundaries to encompass possible impacts the system could have, including interfaces with peer systems, larger systems of which it is a component, and users and maintainers

2. System elements

3. Limiting the system to those elements that affect or interact with each other to accomplish the mission or function

iii. At a minimum, the safety analysis should detail the system and its hazards so that the projected audience can completely understand the associated safety risk. Guidelines that help determine depth include:

1. More complex and/or increased quantity of functions will increase the number of hazards and related causes

2. Complex and detailed analyses will explore multiple levels of hazard causes, sometimes in multiple safety analyses

3. Hazards that are suspected to have associated initial high or medium risk should be thoroughly analyzed for causal factors and likelihood

4. The analysis should be conducted at a level that can be measured or evaluated

D.8 PHASE 2: IDENTIFY HAZARDS.

a) Identifying Hazards. Once the SRM Panel has completely and accurately described the system

(Phase 1), it can identify hazards. A “hazard” is defined as any real or potential condition that can result in injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.

i A thorough system description and the elements within it constitute the potential sources of hazards associated with the proposed change. During the hazard identification phase, the panel identifies and documents potential safety issues, their possible causes, and corresponding effects. The level of detail required in the hazard identification process depends on the complexity of the change being considered and the stage at which the SRM Panel is performing the analysis. A more comprehensive hazard identification process leads to a more rigorous safety analysis.

b) Elements of Hazard Identification. In the “identify hazards phase,” the SRM Panel identifies hazards to the system (i.e., operation, equipment, and/or procedure) in a systematic way. There are numerous ways to do this, but all require at least three elements:

• Operational expertise

• Training or experience in various hazard analysis techniques

• A defined hazard analysis tool

c) The SRM Panel defines the data sources and measures necessary to identify hazards and to monitor for compliance with mitigation strategies. Data monitoring also helps detect hazards that are more frequent or more severe than expected or mitigation strategies that are less effective than expected. Whoever performs the hazard analysis selects the tool that is most appropriate for the type of system being evaluated. Table 1 lists several hazard identification and analysis tools and techniques. These are just some of the many tools that panels can use to identify hazards.

d) Potential Sources of Hazards. The hazard identification stage considers all of the possible sources of hazards. Depending on the nature and size of the system under consideration, these could include:

• Equipment (hardware and software)

• Operating environment (including physical conditions, airspace, and air route design)

• Human operators

- Human-machine interface
- Operational procedures
- Maintenance procedures
- External services

e) The SRM Panel should refer to the system description it created using the 5M Model or other technique. These elements are often the sources for hazards.

f) Documenting Existing Hazards. The “Documenting Existing Hazards” Process describes the documentation and notification actions required when an existing hazard is identified. During Phase 2 of the SRM process, the SRM Panel or change proponent identifies hazards for the system change undergoing the analysis. Those hazards fall into three categories:

- Pre-existing hazards not in scope and not caused by the change
- Pre-existing hazards in scope and not caused by the change
- Hazards in scope and caused by the change

NOTE: Each of these three categories above follows a specific process for ensuring ownership, documentation, and monitoring.

g) The overall objective of any SMS is to improve aviation safety. There may be instances in which a panel discovers existing high-risk hazards through an assurance program, a safety analysis, or other means. In those cases, corrective action is necessary to resolve the identified issue. If the panel is unable to find a corrective action that will meet the requirements for acceptable risk under SRM, it must prove that the corrective action either increases the safety of the system or reduces the safety risk in the system. The panel recommends the corrective action. The implementing party continues to work toward identification of a corrective action that meets the SRM requirements and/or continues to work toward managing the risk down to an acceptable level on the implemented change. This applies to existing hazards only. Likewise, if an SRM Panel identifies existing high-risk hazards in a system, corrective action is necessary. No one should be allowed to introduce new high risk as the result of implementing a new change to a system.

h) Causes, System State, and Effect Defined. During the hazard identification phase, the panel identifies and documents potential safety issues, their possible causes, the conditions under

which hazards might be realized (system state), and corresponding effects. “Causes” are events that result in a hazard or failure, which can occur independently or in combinations. They include, but are not limited to:

- Human error
- Latent errors
- Design flaws
- Component failure
- Software errors

i) A “system state” is defined as the expression of the various conditions, characterized by quantities or qualities in which a system can exist.

j) It is important to capture the system state that most exposes a hazard. The system description remains within the confines of any operational conditions and assumptions defined in existing documentation. System state can be described using one or some combination of the following terms:

- Operational and Procedural—types of operations
- Conditional—Instrument Meteorological Conditions vs. Visual Meteorological Conditions, peak vs. low work volumes, etc.
- Physical—Environmental effects, primary power source vs. back-up power sources, dry vs. contaminated runways, etc.

k) Any given hazard may have a different risk level in a different system state. Hazard assessment must consider all possibilities, from the least to the most likely, allowing for “worst case” conditions. It is important to capture all system states to identify worst credible outcomes and unique mitigations. The SRM Panel must ensure that the hazards to be included in the final analysis are “credible” hazards considering all applicable existing controls. They can use the following definitions as a guide in making such decisions:

- Worst—The most unfavorable conditions expected (e.g., extremely high levels of work, extreme weather disruption)

• Credible—Implies that it is reasonable to expect the assumed combination of extreme conditions will occur within the operational lifetime of the change

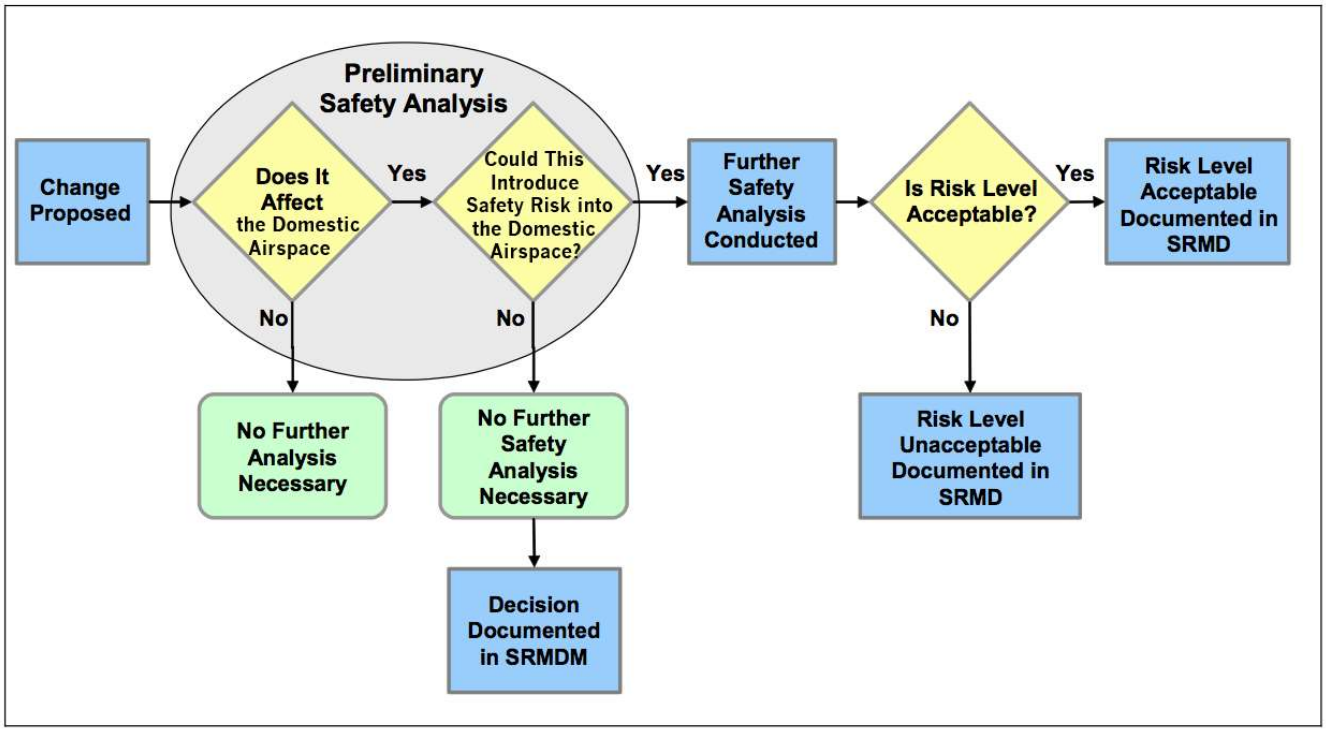
l) The goal of the safety analysis is to define appropriate mitigations for all risks associated with each hazard. While the worst credible outcome may produce the highest risk, the likelihood of the worst credible outcome is often very low. However, a less severe outcome may occur more frequently and result in a higher risk than the worst effect. The mitigations for the two outcomes may be different and both must be identified. It is important for the panel to consider all possible outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.

m) The SRM Panel should consider identifying the accumulation of “minor” failures or errors that result in hazards with greater severity or likelihood than would result if the panel considered each failure or error independently.

n) The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

o) The Bow-Tie Model in Figure 7 illustrates the relationship between causes, hazards, and what kind of environment (system state) enables their propagation into the different effects. While it may be used in conducting a safety analysis, the Bow-Tie model is included here as a means to conceptualize safety risk associated with hazards under various conditions. This model assumes each hazard can be represented by one or many causes, having the potential to lead to one or many effects (incidents or events) in various system states.

Figure 7. The Bow-Tie Model



p) The Bow-Tie model is a structured approach in which causes of hazards are directly linked to possible outcomes or effects in a single diagram. The underlying analysis can be simple or complex depending on what is appropriate for the change being analyzed.

q) For each effect associated with the hazard, one assigns a severity. To understand a hazard's severity, one determines the hazard's cause and the circumstances under which it occurred (e.g., the system state). The same model can be used to help determine the likelihoods associated with the different effects that are the result of a particular hazard given the outlined system states.

r) Tools and Techniques for Hazard Identification and Analysis. The following tools and techniques can be helpful in identifying and analyzing hazards. In many cases, using a single tool or technique will suffice. However, some cases may require multiple tools and techniques. Safety Engineers can provide additional guidance on which tool(s) to use for various types of changes.

s) Table1 describes a selection of hazard identification and analysis tools and techniques.

Table 1. Selection of Hazard Identification and Analysis Tools and Techniques

Tool or Technique	Summary Description
Preliminary Hazard Analysis (PHA)	The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep.
Operational Safety Assessment (OSA)	The OSA is a development tool based on the assessment of hazard severity. It establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced.
Fault Hazard Analysis (FHA)	The FHA is a deductive method of analysis that personnel can use exclusively as a qualitative analysis or, if desired, can expand to a quantitative one. The FHA requires a detailed investigation of the subsystems to determine component hazard modes, causes of these hazards, and resultant effects on the subsystem and its operation.
What-If Analysis	The What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. One can use the What-If Analysis as a brainstorming method.

Tool or Technique	Summary Description
Scenario Analysis	The Scenario Analysis identifies and corrects potentially hazardous situations by postulating accident scenarios in cases where it is credible and physically logical.
Change Analysis	The Change Analysis analyzes the hazard implications of either planned or incremental changes (e.g., operation, equipment, or procedure).
Interface Analysis	One uses the Interface Analysis to discover the hazardous linkages between interfacing systems.
Job Safety Analysis (JSA)	One uses this technique to assess in detail the safety considerations in a single job or task.
Job Task Analyses (JTA)	The foundation of the performance of HEA is a task analysis, which describes each human task/sub-task within a system in terms of the perceptual (information intake), cognitive (information processing and decision making), and manual (motor) behaviors required of an operator, maintainer, or support person. It should also identify the skills and information required to complete the tasks; equipment requirements; the task setting; time and accuracy requirements; and the probable human errors and consequences of these errors. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.

t) Tool Selection Criteria. Some considerations to take into account when selecting hazard identification/analysis tools include:

u) The necessary information and its availability

v) The timeliness of the necessary information and the amount of time required to conduct the analysis

w) The tool that will provide the appropriate systematic approach to:

- Identifying the greatest number of relevant hazards
- Identifying the causes of the hazards
- Predicting the effects associated with the hazards
- Assisting in recommending/identifying effective risk mitigations

D.9 PHASE 3: ANALYZE RISK.

a) Analyzing Risk. In this phase, the SRM Panel:

- Evaluates each hazard (from Phase 2) and the system state in which it potentially exists (from Phases 1 and 2) to determine what controls exist to prevent or reduce the hazard's occurrence or effect(s)
- Compares a system and/or sub-system, performing its intended function in anticipated operational environments, to those events or conditions that would reduce system operability or service

b) These events may, if not mitigated, continue until total system degradation and/or failure occurs. These mitigations are called existing controls. Once the SRM Panel documents the existing controls, it estimates the hazard's risk.

c) An accident rarely results from a single failure or event. Consequently, risk analysis is often not a single binary (on/off, open/close, break/operate) analytical look. While they may result in the simple approach, risk and hazard analyses are also capable of looking into degrees of event analysis or the potential failure resulting from degrading events that may be complex and involve primary, secondary, or even tertiary events.

d) "Risk" is defined as the product of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. The SRM Panel can use quantitative or qualitative methods to determine the risk, depending on the application and the rigor it uses to analyze and characterize the risk. Different failure modes of the system(s) can impact both severity and likelihood in unique ways.

e) Existing Controls. In this phase, the SRM Panel evaluates each hazard and the system context in which the hazard potentially exists to determine what prevents or reduces the hazard's occurrence or mitigates its effects. These mitigations are called existing controls. A control can only be considered existing if it has been validated and verified with objective evidence. Until it is validated, it is considered a recommended requirement.

f) It is important to document existing controls as the panel's understanding of existing controls impacts its ability to establish credible severity and likelihood determinations. When identifying existing controls, the SRM Panel takes credit for controls specific to the change, hazard, and system state.

g) Determining Severity. "Severity" is the measure of how bad the results of an event are predicted to be. One determines severity by the worst credible outcome. The SRM Panel must examine all effects and consider the worst credible severity. One does not consider likelihood when determining severity; determination of severity is independent of likelihood. The goal of the safety analysis is to define appropriate mitigations for all risks associated with each hazard. While the worst credible outcome may produce the highest risk, the likelihood of the worst credible outcome is often very low. However, a less severe outcome may occur more frequently and result in a higher risk than the worst effect. The mitigations for the two outcomes may be different and both must be identified. It is important for the panel to consider all possible outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.

h) Likelihood and Risk Assessment. "Risk" is the product of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state; likelihood is an expression of how often one expects an event to occur.

i) One must consider severity in conjunction with the determination of likelihood. Likelihood is determined by how often one can expect the resulting harm to occur at the worst credible severity.

j) The SRM Panel uses likelihood definitions (in the first three columns) when acquiring new or modifying existing systems. Flight Procedures definitions (in the sixth column) can be used when assessing flight procedures. Safety professionals can use the likelihood definitions for both Systems and Flight Procedures prior to the development and implementation of the SMS.

k) Use of Qualitative and Quantitative Data. In assessing risk, one can use both quantitative and qualitative methods. Using quantitative data is preferred, as it tends to be more objective; however, when quantitative data are not available, it is acceptable to rely on qualitative data

and expert judgment. Qualitative judgment varies from person to person, so if only one person is performing the analysis, the result should be considered an opinion. With a team of experts involved in the analysis, one can consider the result qualitative data or expert judgment.

l) Characteristics of quantitative data include:

- Data are expressed as a quantity, number, or amount
- Data tend to be more objective
- Data allow for more rational analysis and substantiation of findings
- Modeling

m) Modeling techniques, such as event-tree analysis, permit either statistical or judgmental inputs. If modeling is required and data are available, the risk assessment should be based on statistical or observational data (e.g., radar tracks, hours flown, labor hours, etc.). Where there is insufficient data to construct purely statistical assessments of risk, judgmental inputs can be used but they should be quantitative. For example, the true rate of a particular type of activity may be unknown, but can be estimated using judgmental input. In all cases, quantitative measures should take into consideration the fact that historical data may not represent future operating environments. In such cases, some adjustment to the input data may be required.

n) Characteristics of qualitative data include:

- Data are expressed as a measure of quality
- Data are subjective
- Data allow for examination of subjects that can often not be expressed with numbers but by expert judgment

Table 2. Likelihood Definitions using Quantitative Data

	Quantitative
Frequent	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-3}$
	Has occurred several times in our organization
Probable	Probability of occurrence per operation/operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$
	Has occurred several times in the aviation industry
Remote	Probability of occurrence per operation/operational hour is less than $1x10^{-5}$, but equal to or greater than $1x10^{-7}$
	Has occurred in our organization
Extremely Remote	Probability of occurrence per operation/operational hour is less than $1x10^{-7}$, but equal to or greater than $1x10^{-9}$
	Has occurred in the aviation industry
Extremely Improbable	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$
	Has never happened in the aviation industry

D.10 PHASE 4: ASSESS RISK.

a) Assessing Risk. In this phase, the SRM Panel:

• Compares each hazard's associated risk (as identified in Phase 3) and plots the risks on a pre-planned risk acceptability matrix

• Determines a hazard's priority by the location of its associated safety risk on this risk matrix

• Gives higher priority hazards the greatest attention in the treatment of risk

b) Risk Matrix Definition. A risk matrix is a graphical means of determining risk levels. The rows in the matrix reflect previously introduced severity categories, and its columns reflect previously introduced likelihood categories. The SRM Panel assesses risk by using the risk matrix in Figure 8.

c) The risk levels used in the matrix are defined as:

• “High”—Unacceptable risk; change cannot be implemented unless the hazard’s associated risk is mitigated so that risk is reduced to a medium or low level. Tracking, monitoring, and management are required. Hazards with catastrophic effects that are caused by: (1) single point events or failures, (2) common cause events or failures, or (3) 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.

• “Medium”—Acceptable risk; minimum acceptable safety objective; change may be implemented, but tracking, monitoring, and management are required.

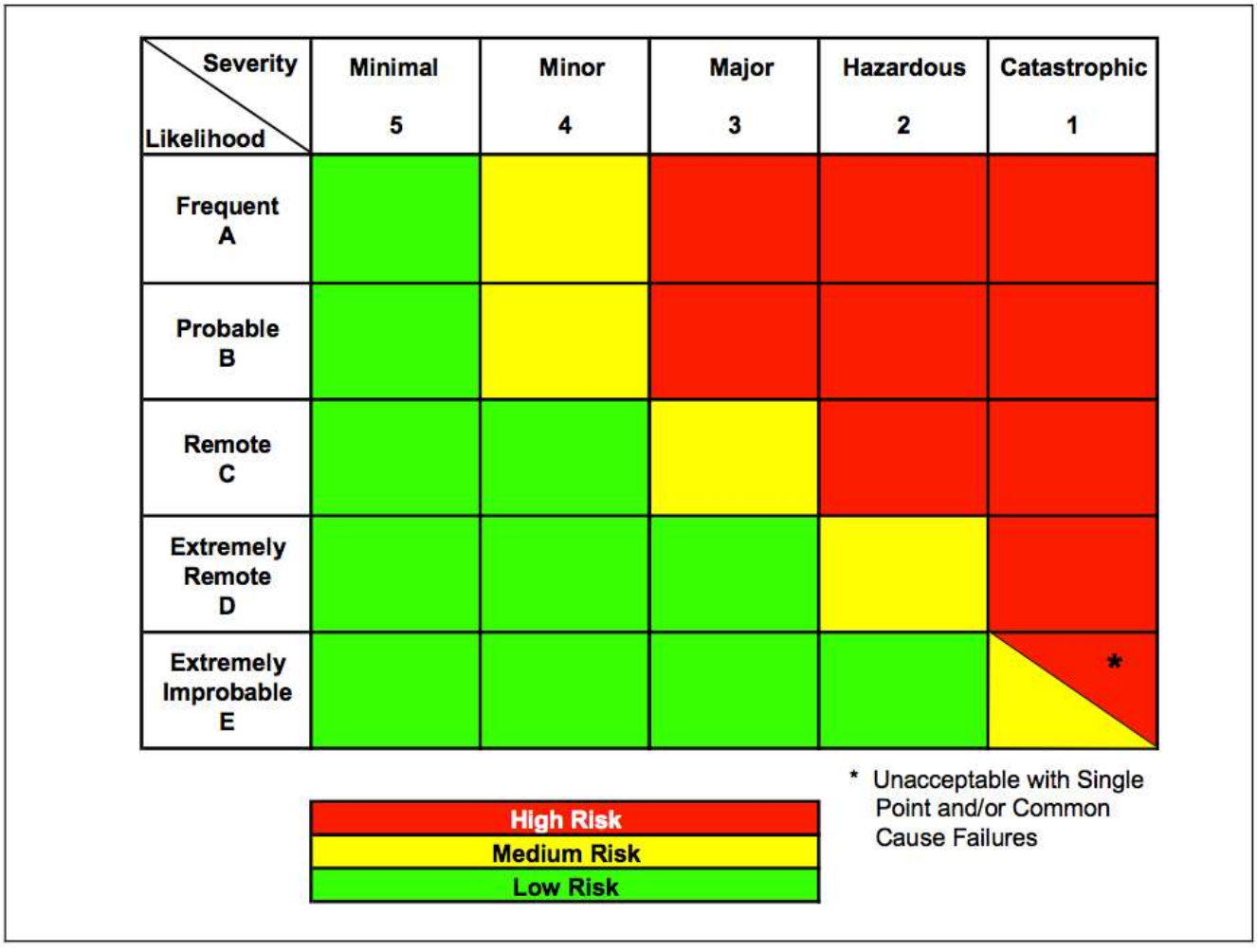
• “Low”—Acceptable without restriction or limitation; hazards are not required to be actively managed but must be documented.

d) A catastrophic severity and corresponding extremely improbable likelihood qualify as medium risk, as long as 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 effect of the hazard is categorized as high risk and placed in the red part of the split cell in the bottom right corner of the matrix.

e) A “single point failure” is defined as a 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. An example of a single point failure is 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 system will fail.

f) A “common cause failure” is defined as a single fault resulting in the corresponding failure of multiple components. An example of a common cause failure is redundant computers running on the same software, which is susceptible to the same software bugs.

Figure 8. Risk Matrix



g) Types of Risk.

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

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

iii. Predicted Residual Risk. Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk

is based on the assumption that all safety requirements will be validated and verified.

iv. Residual Risk. Residual risk is the risk that remains after all control techniques have been implemented or exhausted and all controls have been verified. Only verified controls can be used to assess residual risk.

v. Substitute Risk. Risk unintentionally created as a consequence of safety risk controls.

h) Ranking and Prioritizing Risk for Each Hazard. The SRM Panel follows these guidelines in ranking and prioritizing risk for each hazard:

i. Rank hazards according to the severity and the likelihood of their associated risk (illustrated by where they fall on the risk matrix).

ii. To plot a hazard on the risk matrix, select the appropriate severity and move down to the appropriate likelihood row.

iii. Plot the hazard in the box where the severity and likelihood of the effect associated with the hazard meet.

iv. If this box is red, the risk associated with the hazard is high; if the box is yellow, the risk associated with the hazard is medium; and if the box is green, the risk associated with the hazard is low.

NOTE: Rank the risks associated with the identified hazards prioritizes treatment and mitigation. High-risk outcomes must be mitigated before the proposed change can be implemented.

i) Handling High Risk Hazards. When a High Risk Hazard (HRH) is identified by an SRM Panel or change proponent, the proposed change cannot be implemented until the following conditions have been met:

• The HRH is mitigated to an acceptable level of risk (medium or low)

• The risk is accepted

• The mitigations are approved by upper management

D.11 PHASE 5: TREAT RISK.

a) Treating Risk. In this phase, the SRM Panel develops and manages options to deal with risk (from Phase 4). Effectively treating risk involves:

- Identifying feasible mitigation options
- Developing a risk treatment plan accepting the predicted residual risk
- Developing a monitoring plan detailing review cycles for evaluating the effectiveness of mitigations
- Implementing and verifying the mitigations
- Monitoring the effectiveness of the mitigation

b) In the treat risk phase, the SRM Panel develops alternative strategies for managing the risk associated with a hazard. These strategies become actions that reduce the risk of the hazard's effects on the system (e.g., human interface, operation, equipment, procedures). While the SRM Panel develops options to mitigate risk, it is the responsibility of the organization(s) making proposed change to implement and verify the mitigations, as well as monitor their effectiveness.

c) Risk Mitigation Definition. Risk mitigation is taking action to reduce the risk of the hazard's effects. Examples of risk mitigation include:

- Revising the system design
- Modifying operational procedures
- Establishing contingency arrangements

d) When risk is determined to be unacceptable, the SRM Panel identifies and evaluates risk mitigation measures that would reduce the risk to an acceptable level. Once identified, the SRM Panel assesses how the proposed mitigation measures affect the overall risk. If necessary, the team repeats the process until a combination of measures reduces the risk to an acceptable level.

e) When risk mitigation strategies cross organizational boundaries, those stakeholder organizations should approve documentation and accept risk.

f) If the risk does not meet the predetermined acceptability criteria, it must always be reduced to a level that is acceptable, using appropriate mitigation procedures to implement the change. Even when the risk is classified as acceptable, if any measures could further reduce the risk, the

appropriate party should:

- Make an effort to implement these measures, if feasible
- Consider the technical feasibility of further reducing the risk
- Evaluate all such cases individually

g) Remember that when an individual or organization “accepts” a risk, it does not mean that the risk is eliminated. Some level of risk remains; however, the individual or organization has accepted that the predicted residual risk is sufficiently low to a degree that it is outweighed by the benefits.

h) If SRM Panel members identify systemic hazards, then the impacted managers can identify and implement risk mitigation efforts. Managers should also assess proposed mitigations for possible collateral system impacts and initiate appropriate corrective actions.

i) Risk Mitigation Strategies. Risk mitigation normally requires the appropriate management’s informed decision to approve, fund, schedule, and implement one, or more, risk mitigation strategies. The objective of this phase is to implement appropriate plans to mitigate the risk associated with identified hazards and their effects. The SRM Panel develops, documents, and recommends appropriate risk mitigation strategies. The risk mitigation approach selected may fall into one or more of the following categories:

- Risk avoidance strategy
- Risk transfer strategy
- Risk assumption strategy
- Risk control strategy

j) Once the SRM Panel selects and develops risk mitigation strategies, the appropriate management can identify the impact on other organization(s) and coordinate/obtain agreement on those strategies with the affected organization(s). In addition, the SRM Panel establishes a monitoring plan to ensure that risk mitigation strategies are effective. It repeats the risk mitigation process until risk is reduced to an acceptable level.

k) Hazard tracking is a key element of this risk management phase.

l) Risk Avoidance Strategy. The risk avoidance strategy averts the potential of occurrence and/or consequence by selecting a different approach or by not participating in the operation, procedure, or system (hardware and software) development. SRM Panels may pursue this technique when multiple alternatives or options are available.

m) The risk avoidance strategy is more likely used as the basis for a “go” or “no-go” decision at the start of an operation or program. The avoidance of risk is from the perspective of the overall organization. Thus, an avoidance strategy is one that involves all the stakeholders associated with the proposed change.

n) Risk Transfer Strategy. The risk transfer strategy shifts the ownership of risk to another party. Organizations transfer risk primarily to assign ownership to the organization or operation most capable of managing it. The receiving party must then accept the risk, which must be documented using a Letter of Agreement, Statement of Agreement, Memorandum of Agreement, or other type of document. Examples of risk transfer may include:

- Transfer of responsibility for a function from one party to another
- Development of new policies or procedures to change “ownership” of a particular element to a more appropriate organization
- Contract procurement for specialized tasks from more appropriate sources (e.g., contract maintenance)
- Transfer of systems from the operating organization to an organization that provides services

o) The receiving organization may be better equipped to mitigate the risk at the operational or organizational level. Transfer of risk, while theoretically an acceptable means of mitigating risk, cannot be the only method used to treat high risk associated with a hazard. The SRM Panel must still mitigate the safety risk to medium or low levels before it can be accepted.

p) In addition, when hazards (and associated risks) that are outside the scope of the SMS are identified (e.g., occupational safety, physical, and information security), organizations transfer the management and mitigation of these risks to the appropriate organization.

q) Risk Assumption Strategy. The risk assumption strategy is simply accepting the likelihood or probability and the consequences associated with a risk’s occurrence. It is not acceptable to use an assumption strategy to treat high risk associated with a hazard. The safety risk must still be reduced to medium or low before it can be accepted, as required by SRM documented in this

manual.

r) Risk Control Strategy. A control is anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls must be written in requirement language.

s) A risk control strategy helps to develop options and alternatives and take actions that lower or eliminate the risk. Examples include implementing additional policies or procedures, developing redundant systems and/or components, and using alternate sources of production. When this is done, it becomes a safety requirement. A correct requirement is unambiguous and verifiable. Controls can be complex or simple.

t) Safety Order of Precedence. There is a preferred order for the development of risk mitigation controls:

- Design for minimum risk
- Incorporate safety devices
- Provide warning
- Develop procedures and training

u) Safety professionals use these in relation to system (hardware/software) development and modification. Table 3 shows the safety order of precedence, which reflects this order.

Table 3. Safety Order of Precedence

Description	Priority	Definition	Example
Design for minimum risk	1	Design the system (e.g., operation, procedure, human-to-system interface, or equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level by selecting alternatives.	1. If a collision hazard exists because of a transition to a higher Minimum En Route Altitude at a crossing point, moving the crossing point to another location would eliminate the risk. 2. If "loss of power" is a hazard to a system, adding a second independent power source reduces the likelihood of the "loss of power" hazard.
Incorporate safety devices	2	If identified risks cannot be eliminated through alternative selection, reduce the risk by using fixed, automatic, or other safety features or devices and make provisions for periodic functional checks of safety devices.	1. An automatic "low altitude" detector in a surveillance system 2. Interlocks to prevent exposure to radiation or high voltage 3. Automatic engine restart logic
Provide warning	3	When neither alternatives nor safety devices can effectively eliminate or adequately reduce risk, warning devices or procedures are used to detect the condition and to produce an adequate warning. The warning must be provided in time to avert the hazard's effects. Warnings and their application are designed to minimize the likelihood of inappropriate human reaction and response.	1. A warning displayed on an operator's panel 2. "Engine Failure" light in a helicopter 3. Flashing Minimum Safe Altitude Warning or Conflict Alert Indicator on a radar screen
Develop procedures and training	4	Where it is impractical to eliminate risks through alternative selection, safety features, and warning devices, procedures and training are used. However, management must concur when procedures and training are solely applied to reduce risks of catastrophic or hazardous severity.	1. A missed approach procedure 2. Training in stall/spin recovery 3. Procedure to vector an aircraft above a Minimum Safe Altitude on a Very High Frequency Omni-directional Range airway 4. Procedures for loss of communications

v) Risk Not Sufficiently Reduced. If the risk cannot be reduced to an acceptable level after attempting all possible mitigation measures, then the change does not satisfy the safety requirements. Therefore, the change proponent must either revise the original objectives or abandon the proposed change. If the proposal is unacceptable, the change cannot be implemented. This conclusion must be included in the SRMD.

w) Hazard Tracking. Hazard tracking is a dynamic process in which hazards and their associated

safety risk information and safety requirements are entered into a database. The information is updated throughout the lifecycle of a system or change. Hazard tracking, in part, includes documenting safety requirements, providing the status of requirements validation and verification, verifying implementation, and updating the current and predicted residual risk levels before acceptance. Hazard tracking also assesses the effectiveness of existing and recommended safety requirements in the control of the identified hazards. The purpose of hazard tracking and risk resolution is to ensure a closed-loop process of managing safety hazards and risks.

x) A useful practice is to use a restricted access, web-based system to document all hazards and their associated risk information. All departments within an organization can then use a hazard tracking system provided by the organization to capture all safety hazards. In this manner, organizations formally identify all hazards, and track and monitor all initial medium and high risk hazards for the lifecycle of the system or change, or until they mitigate the risk to low. Organizations can also verify the effectiveness of the controls mitigating all risks through continuous monitoring. If through SRM processes and/or safety assurance measures the mitigations are found ineffective in reducing the risk to an acceptable level, the change proponent and/or SRM Panel should reassess the risk and implement additional mitigations until further monitoring illustrates the risk is mitigated to low. Hazards with low associated risk by definition can be considered to meet the organization's safety requirements for target level and may not require further mitigation.

y) A key principle of the SMS is that SRM and safety assurance are integrated. Through the SRM process, an organization can develop safety risk mitigations and monitoring plans. Through safety assurance processes, the organization monitors those mitigations and identifies new hazards or necessary changes, which must go through the SRM process. Hazard tracking is a means to ensure that these two SMS components function together to manage safety risk.

z) Training and Access to HTS. It is a good practice to use a Hazard Tracking System (HTS) to track hazards. An HTS can be a secure web site housed behind a firewall. In some systems, there are two separate HTS interfaces – one for systems acquisitions/engineering and one for operations. Company employees often can obtain access to, or training on, such a system by contacting their department's Safety Manager or Safety Engineer.

aa) Developing a Control Implementation/Monitoring Plan. In addition to tracking the hazards, the SRM Panel develops a plan to:

- Verify the risk mitigations

• Monitor the effectiveness of those mitigations

• Conduct the post-implementation assessments to verify the results of the analysis

Table 4. Sample Recommended Control Implementation/Monitoring Plan

Task	Responsible	Due Date/ Frequency	Status
Implementation of Controls			
The recommended mitigation that was designed for the change	Individual, division, or organization required to render account concerning the identified task	The date by which the responsible party must have completed the identified task	The state of the task
Example: Safety device X will be installed in Equipment Z.	Example: Equipment Technicians	Example: December 5, 2011	Example: Open*
Monitoring			
A function to be performed; an objective	Individual, division, or organization required to render account concerning the identified task	The frequency that the task will be performed	The state of the task
Example: Internal audit of the maintenance records	Example: Quality Assurance Office	Example: Monthly, quarterly, etc.	Example: Ongoing*, Closed

NOTE: * "Open" meaning that the due date of the task has not arrived; "Closed" meaning that the task has been completed (generally one would want to include the date of task completion). Sometimes the task is considered to be "Ongoing", meaning that the task is to be performed throughout the lifecycle of the system.

bb) It is normally required that employees formally monitor all initial medium and high risk hazards for the lifecycle of the system or change, or until they mitigate the risk to low and verify the effectiveness of the controls mitigating the risk. After mitigations have been verified through

monitoring and a target level of risk has been achieved, the change proponent can continue current/existing monitoring and evaluation processes, so that the change becomes the standard operating procedure.

cc) Safety professionals conduct post-implementation assessments for the life of the system or change, as defined in the SRMD monitoring plan. The frequency of assessments depends on the type, the potential safety impact, and/or the complexity of the change, as well as the depth and breadth of the original analysis. Inclusive in these assessments is updating the SRMD; existing support mechanisms should be considered. These support mechanisms may include Independent Operational Test and Evaluation groups, Flight Inspection departments, an Air Traffic Evaluation and Auditing Program, and SRM audits.

D.12 SAFETY RISK MANAGEMENT DOCUMENT (SRMD).

a) SRMD: Tool for Decision Making. An SRMD thoroughly describes the safety analysis for a proposed change. It documents the evidence to support whether the proposed change to the system is acceptable from a safety risk perspective. The SRMD also contributes (from a programmatic or management perspective) to the decision to implement a change. The department responsible for implementing the change maintains all documentation associated with the SRM process, including the SRMD, for the lifecycle of the system or change.

b) The SRMD is a living document that may be modified during the lifecycle of the program.

c) SRMD Contents. An SRMD provides sufficient detail about a proposed change to a current system or the introduction of a completely new system into an operation or larger overall system. It should be a single source that enables the management personnel to understand the change, its associated risks, and corrective steps taken (or proposed) to reduce the initial and subsequent residual risks to an acceptable level. The document must stand alone (i.e., it must contain sufficient detail about the current or proposed system to enable the reader to comprehend what steps have been taken to identify safety issues and the corrective steps taken (or proposed)).

d) An SRMD contains, at a minimum:

i Identification of the system to be introduced or changed, including:

- A description of the current system and proposed change or introduction

• Current controls in place

• Pertinent interfaces and support systems required by the introduction and/or change to function properly

• Reference to any SRMDs submitted on the current system or changes being analyzed

• A statement reflecting the impact of the change or introduction (local, regional, national, etc.)

ii Identification of hazards and causal factors

• Description of methodology and tools used

• Existing controls affected by the introduction and/or change proposed

• The hazards and scenarios and/or circumstances where they exist

iii Analysis, assessment, and mitigation of the associated risks

• Documentation of the identified risks including: Initial risk level (in terms of severity and likelihood), when and how they appear in the current or proposed system If associated with existing risks and/or controls, and how the introduction of a new system or change in the existing system affects the risk

• Controls (mitigations) and their effect on identified risks

• Predicted residual and accepted risks

• Documentation of how the risks and their associated controls will be tracked and monitored throughout the lifecycle of the system or change

iv Strategy for validation and verification of the proposed change or introduction

• Means that will be used to obtain measurable data to monitor the effectiveness of the control

o Who will be responsible for reporting, collecting, and analyzing the data

o How the data will be analyzed

- Means that will be used to determine if adjoining systems are adversely affected
    - Who will be responsible for reporting, collecting, and analyzing the data
    - How will the data be analyzed
- What will determine that safety requirements (existing and recommended) are met and satisfied
- Future plans for updating the present SRMD

e) The SRM Panel documents any change that could have safety consequences in the provision of safety-related services. The scale of an SRMD varies depending on the type and complexity of a proposed system change.

f) The level (i.e., system-wide, regional, or local) at which SRM is initiated may vary by organization or change proponent. If the change is at the regional or local levels, two methods for documenting SRM can be used:

- Address the change in a system-wide SRMD through site-specific parameter ranges
- Develop and append a local-level SRMD to the larger, system-wide SRMD

g) While panels strive to reach consensus, there may be instances in which not all panel members agree on the results of the safety analysis. In that case, the results are documented, ensuring that the opinions of dissenters are also captured and delivered to the decision-maker.

h) The SRMD should be written so that it can be understood by a reviewer familiar with the discipline(s) relevant to the change (e.g., ATC controller, chief pilot, chief inspector, operations manager, chief dispatcher). There should be enough detail that a reviewer unfamiliar with the program, project, or organization can understand the change and the system within which it is contained. The SRMD should include thorough descriptions of the identified hazards and provide rationales for the panel's severity and likelihood assessments for each hazard. Using the SRMD Review Checklist for quality control will minimize delays caused by clarifications requested by SRMD reviewers and approvers. Furthermore, the originating facility/organization assigns SRM documentation numbering when drafting the document. Not all qualifiers will apply to every change; the facility/organization uses each type only when applicable.

i) Additional Resources for SRMD Development. In many instances, existing safety and system engineering processes produce documents that SRM Panels use to support the analysis portion of an SRMD.

j) SRMD Benefits. An SRMD provides a standardized approach to developing a safety case that:

- Reduces omissions and inconsistencies in safety analysis preparation and conduct
- Eases documentation development
- Makes the sharing of safety risk data more manageable
- Strengthens SRM skills
- Encourages a safety culture
- Ensures operational safety data are monitored to reduce hazards
- Provides assurance to decision-makers that SMS processes are being followed
- Establishes responsibility/accountability
- Makes the process repeatable and reduces re-study of similar change proposals

k) Difference Between Risk Acceptance and SRMD Approval. Approving the SRMD means that the approving party agrees that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

i. Accepting the safety risk is a certification by the appropriate manager that he understands the safety risk associated with the change and he/she accepts that safety risk.

ii. Both approving the SRMD and accepting the safety risk are necessary, along with other inputs (e.g., costs, benefits), before implementing a change in a major system.

D.13 SRMD APPROVALS.

a) SRMD Approval Level Requirements. SRMD approvals depend on the span of the program, its associated risk(s), the mitigation(s) used to control the risk, and other regional-specific

guidance. “SRM Documentation Approval” is certification that the documentation was developed properly, hazards were systematically identified, risk was appropriately assigned, suitable mitigations were proposed, and a sound implementation and monitoring plan was prepared. SRMD approval does not constitute acceptance of the risk associated with the change or approval to implement the change.

b) The approval and review of an SRMD follows a process for establishing and maintaining quality assurance for the review and evaluation of SRM documentation. The SRM Panel should involve the approving authority early in the SRM process to obtain agreement on the assumptions and processes that it will use. The level of approval required for an SRMD will be based on the nature of the change and the risk identified.

NOTE: The approval of the SRMD that is described here is an activity that takes place with the aviation organization’s management system and IT DOES NOT, NOR SHOULD IT involve GACA personnel.

c) Post SRMD Approval. The change proponent should retain a copy of the SRMD for the lifecycle of the system or change. Upon request, the proponent of the change should provide their management with copies of SRMDs. SRMDs may also serve as inputs to existing approval processes.

d) SRMDs Related to Changes Not Approved or Implemented. SRMD should be kept on file even if it is not approved or if the change is not implemented. Employees can use this information in assessing similar change proposals or as inputs to SRMDs for other change proposals. SRMDs that are not approved, or those used by a decision-maker in his/her decision not to implement a change, also provide proof that the SMS is performing its intended function (i.e., reducing the safety risk in the civil aviation environment). Relevant oversight entities may also audit this documentation.

e) SRMD Lifecycle. The results of safety analyses are a part of the system baseline information. Company employees may need to update or change an SRMD as a project progresses and as they modify decisions. Safety monitoring may indicate that the controls are less effective than originally expected or that additional hazards exist, which may require additional mitigations. Any change that may affect the assumptions or hazards identified in the SRMD or the estimated risk necessitates an amendment to the SRMD.

f) In addition, the SRMD includes a monitoring plan to conduct post-implementation

assessments to verify the results of the previous analyses and update the SRMD. While necessary for the life of the system or change, the periodicity of these assessments may vary depending on the type, potential safety impact, and/or complexity of the change, as well as the depth and breadth of the original analysis.

g) When developing the plans to monitor the change and update the SRMD, existing support mechanisms should be taken into account. Based on the results of audits and evaluations of how the system performs, an organization may need to modify the SRMD, which could include reopening the safety analysis for additional assessment. The Safety Assurance portion of an SMS should further describe these processes.

D.14 ACCEPTING RISK.

a) Effect of SRM on Safety Levels. Through SRM, decision-makers knowingly accept risk and thus are better able to manage it; this leads to increased safety. Understanding the consequences of risk increases the ability to anticipate and control the impacts of internal and/or external events on a program.

b) Accepting Safety Risk. Risk Acceptance is the certification by the appropriate management official that he/she understands the safety risk associated with the change, the mitigations are feasible and will be implemented, and he/she accepts that safety risk into the civil aviation environment.

c) Accepting the safety risk is a prerequisite to making a proposed change. Risk acceptance is based on predicted residual risk. Accepting the safety risk is different from approving an SRMD.

d) Approving an SRMD indicates that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

e) Authority to Accept Safety Risk. The acceptance of the safety risk depends on the span of the program or change, its associated risk, and the mitigation used to control the risk. Only those responsible for the change and in a position to manage the risk can accept the risk into the civil aviation environment.

f) Changes that have high, medium, or low initial safety risk, some of which have been mitigated

to lower levels will need to be managed by an appropriately high level of management.

D.15 TRACKING CHANGES.

a) Change Tracking. In addition to the SRMDM and SRMD, each department within an organization should maintain a tracking matrix containing proposed system changes within its purview and the related outcome. Table 5 provides an example of a form that departments can use as a system Change Tracking Matrix and the minimum information that is recommended.

Table 5. Example of a Change Tracking Matrix

	Information Regarding the Change					Safety Risk Management Information				
Service Unit	Date Change Proposed	Title of Change	Narrative Description of Change	Accountable Office	Change Approved by	SRMD or SRMDM Developed	Date of SRMD or SRMDM	SRM Point of Contact	SRMD or SRMDM Approved by	Risk Accepted by

b) Change Tracking Matrix Responsibilities. Safety personnel review and analyze the data provided in the sample Change Tracking Matrix, and when appropriate, provides feedback to the organizations concerning their use of SRM. This analysis assists in identifying the scope of the SRM effort, as well as identifying the resources required to conduct SRM. Safety personnel then share the information with upper management; this information helps upper management identify the scope of its oversight effort and provides insight into the processes used by the organization to improve the safety of the civil aviation environment. In addition, each department is responsible for maintaining its own Change Tracking Matrix and providing monthly updates to Safety personnel.

c) Before Implementing a System Change. In addition to SRM, upper management verifies that a new or modified system (hardware and software) is ready for use in the operational environment for which it is intended. Specifically, the team responsible for the system conducts test and evaluation before implementing a system or a change to the system. It determines the method of verification based on the nature of the change. Through verification, the team shows that the system meets its requirements and performs its intended function(s).

d) Methods of verification include test, analysis, examination, and demonstration/evaluation. In

addition to verification by the implementing department, Safety personnel conduct an independent assessment of operational readiness on designated systems prior to the in-service management phase.

e) SRM Resources. Each relevant department should have a designated Safety Manager who can provide additional guidance regarding the SMS and SRM. In addition, each relevant department should have a Safety Engineer who provides SRM expertise. Both the Safety Manager and Safety Engineer should also be available to provide input to the management personnel who will accept the risk associated with the change. In addition, if risk is to be accepted outside the department, the Safety Manager and/or Safety Engineer help facilitate that coordination.

Figure 9. Glossary

ATC Air Traffic Control

ATCT Air Traffic Control Tower

CSA Comparative Safety Assessment

ETBA Energy Trace and Barrier Analysis

FHA Fault Hazard Analysis

FMEA Failure Mode and Effect Analysis

FMECA Failure Modes, Effects, and Criticality Analysis

FTA Fault Tree Analysis

GACA General Authority of Civil Aviation

HAZOP Hazard and Operability Tool

HEA Human Error Analysis

HRH High Risk Hazard

HTS Hazard Tracking System

JSA Job Safety Analysis

JTA Job Task Analyses

MORT Management Oversight and Risk Tree

OSA Operational Safety Assessment

PHA Preliminary Hazard Analysis

PHL Preliminary Hazard List

SMS Safety Management System

SRMDM SRM Decision Memo

SRM Safety Risk Management

SRMD Safety Risk Management Document

SSAR System Safety Assessment Report