Developmental Guidance for

DESIGN AND MANUFACTURING

SAFETY MANAGEMENT SYSTEM FRAMEWORK

REVISION D

For:

D&M SMS Pilot Project Participants and Voluntary Implementation of SMS Programs

Federal Aviation Administration

Aircraft Certification Service – MSMS Project

November 14, 2011

Record of Changes

Revision	Date	Pages/Sections Affected	Description of Revision
A	2/24/2011	19-20 / Sub-Element 2.1.1	New Sub-Element clarification content added
B	04/08/11	All sections	Completed a technical edit on the entire document that refined grammar, acronyms, abbreviations and punctuation. No substantive content changes were made.
C	09/12/11	Multiple pages and sections	- 1.1(2)(e) intent guidance added - 1.1(2)(f) intent guidance and examples added - 1.1(2)(j) timeframe guidance added; intent guidance added - 1.1(5) added example info - 1.2(2) added SMS output examples - 1.2(3) added SMS outputs examples - 1.3(1) added clarifying intent info - 1.3(2) added SMS output example - 1.3(3) added SMS output example - 2.1.2 added example hazards - 2.2(3) added method of meeting expectation - 2.2.3 added SMS output example - 3.1.1 added example hazards and associate indicators - 3.1.7 (eliminated improper reference) - 3.1.7(5) added clarification for expectation - 3.1.8 added clarification to expectation - 4.1.1(1-2) added SMS output example - Corrected typo in Framework section 4.2(6) (added missing word)
D	11/14/11	Multiple pages and sections	Added information that is now considered guidance from previous version of the Framework.

Introduction

The Federal Aviation Administration (FAA) Aircraft Certification Service (AIR) has produced this Developmental Guidance (DG) document to provide assistance to an organization so that it can develop its Design and Manufacturing (D&M) Safety Management System (SMS) using the D&M SMS Framework. This document presents the text for each Framework building block or standard (STND), which is outlined by a box labeled as such. Each STND is followed by a Developmental Guidance section labeled (DG) containing further explanation and, where appropriate, one or more examples.

D&M SMS Framework Overview

The D&M SMS DG document replicates the structure of the D&M SMS Framework's functional expectations using a hierarchical structure of components, which are composed of elements and their subordinate sub-elements. The D&M SMS Framework structure employs the four basic components of a safety management system: Safety Policy and Objectives, Safety Risk Management, Safety Assurance, and Safety Promotion. The structure of the D&M SMS Framework building blocks used in the DG document is outlined in the following sections.

a. Safety Policy and Objectives (Component 1.0)

Effective management systems must define policies, procedures, and organizational structures to accomplish their goals. The SMS Framework's Safety Policy and Objectives Component outlines expectations in the Elements below, which in turn provide the foundation for the functional SMS Components 2.0 and 3.0 (Safety Risk Management and Safety Assurance).

- Safety Policy (Element 1.1)
- Management Commitment and Safety Accountabilities (Element 1.2)
- Key Safety Personnel (Element 1.3)
- Emergency Preparedness and Response (Element 1.4)
- SMS Documents and Records (Element 1.5).

b. Safety Risk Management (Component 2.0)

Safety Risk Management (SRM) is a formal system of hazard identification and analysis and risk control (sometimes termed "mitigations") used to assess systems at both the organizational and product levels. SRM Framework Elements are essential in controlling risk to acceptable levels and their subordinate Sub-Elements are:

- Hazard Identification and System Analysis (Element 2.1)
  - System description and analysis (Sub-Element 2.1.1)
  - Identify hazards (Sub-Element 2.1.2)
- Risk Assessment and Control (Element 2.2)
  - Analyze safety risk (Sub-Element 2.2.1)
  - Assess safety risk (Sub-Element 2.2.2)
  - Control/mitigate safety risk (Sub-Element 2.2.3).

c. Safety Assurance (Component 3.0)

Once SRM controls are identified and employed, an organization must ensure that the SRM-designed and implemented controls continue to be implemented as intended and are effective as the environment changes. The Safety Assurance (SA) function provides for this, using system safety and quality management concepts and sub-elements. SA Framework Elements for assuring safety and the subordinate Sub-Elements are:

- Safety Performance Monitoring and Measurement (Element 3.1)
  - Continuous monitoring (Sub-Element 3.1.1)
  - Internal audit (Sub-Element 3.1.2)
  - Internal evaluation (Sub-Element 3.1.3)
  - Investigation (Sub-Element 3.1.4)
  - Employee reporting and feedback system (Sub-Element 3.1.5)
  - Analysis of data (Sub-Element 3.1.6)
  - System assessment (Sub-Element 3.1.7)
  - Management review (Sub-Element 3.1.8)
- Management of Change (Element 3.2).

d. Safety Promotion (Component 4.0)

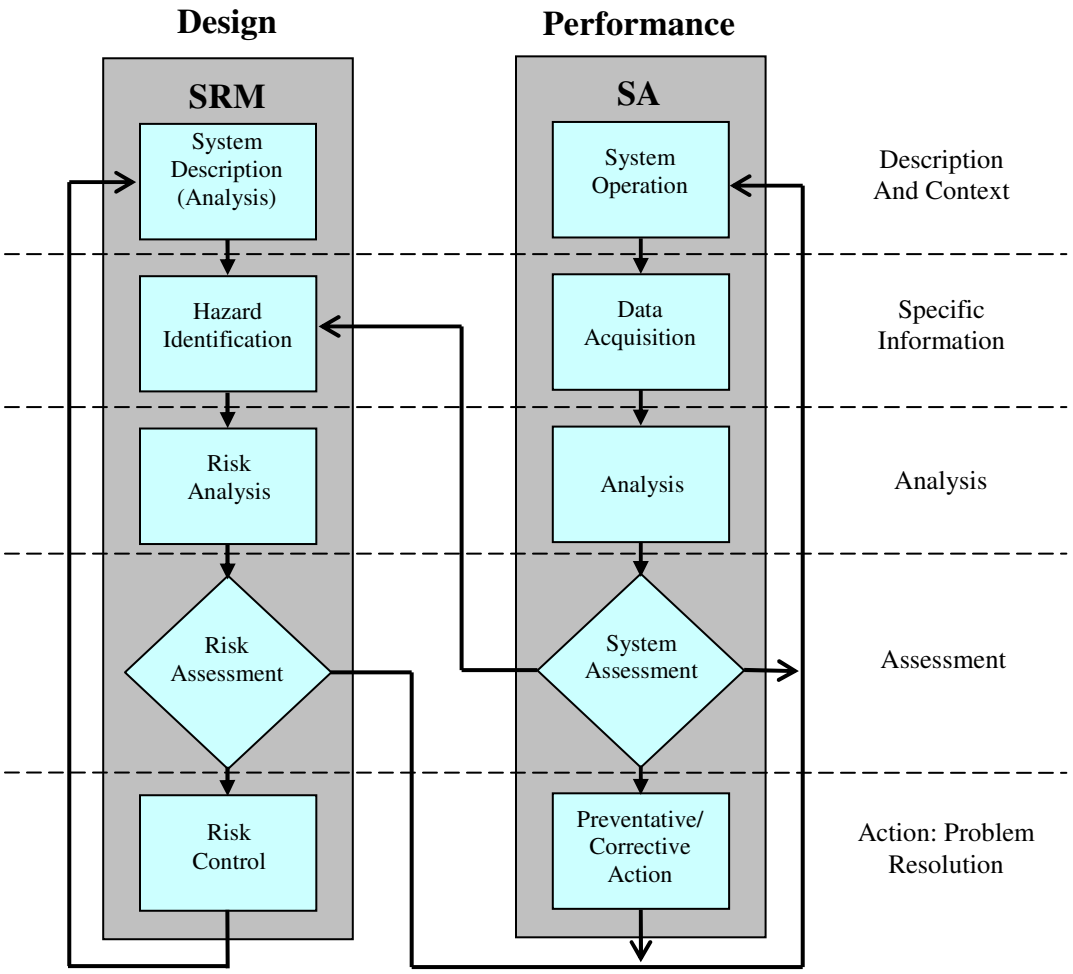
The organization's upper management must promote safety as a core value with practices that support a sound safety culture. The organization must make every effort to communicate its goals and objectives as well as the current status of the organization's activities and significant events. The Safety Promotion Component provides the SMS Framework expectations for establishing and implementing these functions through the following Elements:

- Competencies and Training (Element 4.1)
  - Personnel expectations (competence) (Sub-Element 4.1.1)
  - Training (Sub-Element 4.1.2)
- Communications and Awareness (Element 4.2).

e. Integration of SRM and SA

Once SRM organizational and product risk controls are developed and determined to be capable of bringing the risk to an acceptable level, they are employed operationally. Then the SA function takes over to ensure that the risk controls are implemented and continue to achieve their intended objectives. The SA function also provides for assessing the need for new controls because of changes in the operational environment. However, some identified risks may not need controls, but only monitoring because of the improbability of their occurrence. The risk analysis should ascertain when monitoring is a sufficient response, when risk mitigation or control activities are the appropriate responses to an identified risk, or when a product or process change is needed. Figure 1 shows how the SRM and SA functions relate to one another when SRM leads to the need for risk controls.

FIGURE 1. Relationship between SRM and SA Processes



1. Safety Policy and Objectives

1.1 Safety Policy

(STANDARD)

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

(1) Top management will define and sign the organization's safety policy.

(2) The safety policy will:

(a) Include a commitment to implement, maintain and improve the SMS;

(b) Include a commitment to identify and comply with legal and regulatory requirements;

(c) Include a commitment to encourage employees to report safety issues without reprisal (as per Sub-Element 3.1.5);

(d) Establish clear standards for acceptable operational behavior for all employees;

(e) Establish the organization's safety objectives;

(f) Include a commitment to fulfill the organization's safety objectives;

(g) *{Paragraph removed – duplication}*

(h) Be communicated with visible management endorsement to all employees and responsible parties;

(i) Be reviewed periodically to ensure it remains relevant and appropriate to the organization; and

(j) Identify responsibility and accountability of management and employees with respect to the organization's safety objectives.

(k) *{Paragraph removed – duplication}*

(l) *{Paragraph removed – duplication}*

(3) {Paragraph moved to DG}

(4) {Paragraph moved to DG}

(5) {Paragraph moved to DG}

(DEVELOPMENTAL GUIDANCE)

[Corresponding cross reference to NPRM Part 5: 5.3, 5.21, 5.23, 5.25, 5.27, 5.53 to 5.75, 5.95 & 5.97]

1.1(1) – *For any system to function properly, it should be strategically designed, organized, and directed to meet predetermined goals and objectives. The organization's policy defines these goals and objectives to reflect the organization's products, and services as a whole. Top management should widely disseminate its policies, either in written or electronic form, so that all employees are informed of the organization's expectations.* *[Part 5.21(c) & 5.25(b)(2)]*

1.1(2)(b) – *Legal and regulatory requirements are different in that legal requirements may be enacted at any level of government whereas regulatory requirements as used here are governmental orders enacted by a federal agency. Both carry the force of law. [Part 5.3(c)]*

1.1(2)(c) – *Safety information should never be withheld, regardless of its nature, as it can have dire consequences in the world of safety management. It is important that all employees, including those who have a fear of sharing or lack the desire to share, feel comfortable and motivated to share safety information. In order to enable this, all organizations should adhere to a 'no reprisal' policy as it helps to create an atmosphere that fosters the free flow of information and builds trust between management and employees. Organizations can further engrain this commitment to safety in the organizational culture through demonstrations ranging from a simple written expression of managerial commitment to an active cultivation of the free exchange of safety information via an "open door policy." [Part 5.21(a)(4)]*

1.1(2)(d) – *Acceptable operational behavior in this context is defined as both the organization and each individual employee acting with a sense of honesty, responsibility, and accountability towards safety. In short, safety is **every employee's** responsibility. [Part 5.21(a)(5)]*

1.1(2)(e) – *Management should provide information to its employees about creating "doable" and achievable safety objectives. [Part 5.21(a)(1)]*

1.1(2)(f) – *Management should also provide guidance on how to review performance of safety objectives. This guidance can include review methods, frequency, individuals involved, etc. [Part 5.21(a)(2), 5.23(a)(2) & 5.25(a)(4)]*

1.1(2)(j) – *A yearly review generally would be considered sufficient to ensure the responsibilities and accountabilities remain accurate in light of any change in the organization's safety objectives.*

The organization must identify those positions that have an impact on its safety objectives. Employees must understand that what they do impacts the organization's safety objectives. Organizations may choose whether or not their employees have input into setting the organization's safety objectives. [Part 5.23(a)]

1.1(2)(k) – *The scope and lifecycle of the organization's system are two dimensions of an SMS. Scope pertains to **which** departments, divisions, product lines, or similar measures of extent are included in the SMS. Lifecycle pertains to the development, implementation, maintenance, and retirement of an organization's policies, structures, procedures, and processes.*

Organizations use system descriptions to help establish the boundaries of their SMS's. While some organizations may consider their entire organization within the bounds of their SMS's, others may not be so structured. A safety management plan presupposes that a system description is in place. Thus, a system description is not

a part of the plan per se, though it is foundational to the plan (see 2.1.1 System Description and Analysis for more information).

Due to the dynamic nature of a business environment, the safety management plan always needs to be reevaluated for currency and relevance. This is usually done on an annual basis. Regardless of the chosen interval of the evaluations, the proactive aspect of the plan should remain constant. [Part 5.3(a) & 5.21(a)(1)]

1.1(3) – *The organization should establish and maintain procedures with measurable criteria to accomplish the objectives of the safety policy. Measurable criteria are used to determine whether the objective was achieved. Examples of measurable criteria include the number of quality escapes, the changed failure rate of a part, or the number of exceedances prevented. Examples of organizational measurement criteria include: employee process knowledge (measuring awareness of process changes) and awareness of corporate policy (measuring awareness of internal policy and procedures).*

Measures are not expected for each procedural step. However, measures and criteria should be of sufficient depth and level of detail to ascertain and track accomplishment of objectives. Criteria and measures can be expressed in either quantitative or qualitative terms. [Part 5.73(a), 5.53 through 5.75]

1.1(4) – *The organization should establish and maintain supervisory and operational controls to ensure procedures are followed for safety-related operations and activities. Examples of supervisory and operational controls for safety-related operations and activities may include audits to existing policies and procedures, the requirement for management concurrence on a particular risk acceptance, requirement for training certifications for inspectors, and the minimum number of risk analysts on staff organization-wide. [Part 5.21(a)(5)]*

1.1(5) – *The organization should establish and maintain a current safety management plan to describe how it will achieve its safety objectives. A safety management plan is the tool that captures in a practical way what is to be accomplished, by whom it is to be accomplished, and when it is to be accomplished. Typically, it includes:*

- *Purpose and scope*
- *Safety goals and objectives (may be delineated down to specific departments – it is important for organizations to aim for goals that are attainable);*
- *Planned activities designed to accomplish the objectives;*
- *Milestones, timelines, and/or deadlines; and,*
- *Roles and responsibilities by department or individual, as applicable.*

The plan is comprised of safety-related activities, all coordinated toward the achievement of a unified goal or objective. An organization may choose to develop a single organization-wide plan or many departmental level plans to support the common organizational safety objectives. [Part 5.21(d), 5.73(a), & 5.95]

1.2 Management Commitment and Safety Accountabilities

(STANDARD)

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

(1) The organization will appoint an accountable executive that will have the ultimate accountability for the SMS.

(2) Top management will provide resources essential to implement and maintain the SMS.

(3) *{Paragraph removed - duplication}*

(a) {Paragraph removed - duplication}

(b) {Paragraph moved to DG}

(c) {Paragraph moved to DG}

(4) The organization will define levels of management that can make safety risk acceptance decisions as described in Element 2.2(2).

(5) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)

[Corresponding cross reference to NPRM Part 5: 5.21, 5.23, 5.25]

1.2(1) – *Organizational structure often provides the order necessary for the coordination of activities so that an organization can reach its stated goals. Assignment of clear roles, responsibilities, and authorities to the various levels and segments within that organizational structure is a prerequisite for the organization's top management to effectively direct and control an organization's activities. These activities include activities that assure the SMS functions work as planned. [Part 5.25]*

1.2(2) – *The resources necessary for the 'care and feeding' of an SMS are meant to include those beyond the obvious ones of human resources, information technology, time, etc. For example, a risk control may take time to yield meaningful data on its usefulness and effectiveness. It will take people guiding others over time to establish and maintain an internal 'safety culture.' Consequently, top management, through its decisions on resource allocation, will impact the effectiveness of its SMS in a very significant way.*

Management should also consider the chosen organizational structure itself as an asset or resource. Solutions to problems in reaching stated goals are sometimes obtained by way of refinements in, or alterations to, the organizational structure. An organization should pay particular attention to how well its structure facilitates communication between and within its various departments.

It is important to note that the implementation of an SMS differs from the maintenance of an SMS. This distinction recognizes that an SMS can grow and mature over time. The implementation phase is just the beginning, the 'standing up' phase, of an SMS. The maintenance phase involves the routine day-to-day functionality as well as refining, inspecting, fixing, redesigning, etc. Consequently, an organization new to SMS may fully expect that its first generation SMS will evolve and therefore function differently years later.

A Safety Management Plan, Implementation Plan, Resource Management Plan, or Resourced Schedule are all possible ways of addressing this expectation.
[*Part 5.21(a)(3), 5.25(a)(3) & 5.25 (b)(1)]*

1.2(3) – *Employees need to know who is obligated or responsible for what, who is authorized to do what, and who has delegated authorization to do what, etc. Documenting these aspects of the safety-related positions will bring clarity to an organization and can promote efficient business operations. Organizational charts with associated documentation describing organizational responsibilities and authorities are useful tools here when kept current and well-distributed within the employee ranks. Roles and Responsibilities documentation may also be used.*
[Part 5.21(c) & 5.23(a)]

1.2(4) – *This expectation establishes the need for policy to address which level(s) of management make which safety acceptance decisions. The actions to carry out the policy are defined in Sub-Element 2.2.(2)(d). Not all management representatives will be authorized to make every safety decision. Decisions requiring higher level signature may include, but are not limited to, those that involve significant safety risk acceptance, those where the chosen risk mitigation is to be applied to an initially high-risk situation, and those mitigations that might be especially costly. [Part 5.23(b)]*

1.2(5) – *If the organization has a quality policy and/or system, top management should ensure that the quality policy and/or system are consistent with the SMS. The organization can use the Quality Management System (QMS) as a platform on which an SMS can be built. That is, the QMS determines what methods and criteria are needed to obtain measurable quality in the product or service of the organization. An SMS introduces a risk management dimension: what are the chosen methods of risk management and what are the most effective methods of risk management in providing that quality product or service?*

So, if an organization is registered under the International Standards Organization (ISO) (e.g., when an organization is ISO 9001 registered), the organization has a documented quality policy already. That quality policy may or may not include the necessary safety policy from this SMS framework. If not, safety policy would need to be introduced.

1.3 Designation and Responsibilities of Required Safety Management Personnel

(STANDARD)

(1) The organization must identify an accountable executive who, irrespective of other functions, satisfies the following:

(a) Is the final authority over operations associated with the organization's certificate/approval(s);

(b) Controls the financial resources required for the operations associated with the organization's certificate/approval(s);

(c) Controls the human resources required for the operations associated with the organization's certificate/approval(s);

(d) Retains ultimate responsibility for the safety performance of the operations associated with the organization's certificate/approval(s).

(2) The accountable executive must accomplish the following:

(a) Ensure that the SMS is properly implemented and performing in all areas of the organization;

(b) Develop and sign the safety policy of the organization;

(c) Communicate the safety policy throughout the organization;

(d) Regularly review the organization's safety policy to ensure it remains relevant and appropriate;

(e) Regularly review the safety performance of the organization and direct actions necessary to address substandard safety performance in accordance with Sub-Element 3.1.8.

(3) The accountable executive must designate a management representative who, on behalf of the accountable executive, must be responsible for the following:

(a) *{Paragraph moved to DG}*

(b) Facilitating hazard identification and safety risk analysis;

(c) Monitoring the effectiveness of safety risk controls;

(d) Ensuring safety promotion throughout the organization per Component 4.0;

(e) Regularly reporting to the accountable executive on the SMS's performance and on any need for improvement.

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.25]

1.3(1) – *Top management (which can be a person or group of people) has the ultimate responsibility for the SMS and should provide the resources essential to implement and maintain the SMS. Top management needs to appoint a member of management, such as the Safety Manager, who has the responsibilities and*

authority outlined above in the Framework. This person may have other responsibilities in addition to those outlined above and may not necessarily be required to take on this position full-time. In the interest of maximizing accountability, the expectation is that all the responsibilities outlined above reside in one person rather than being distributed to two or more people.

Element 1.2 states an executive must be named for the purpose of ultimate accountability of the SMS. In this Sub-Element, more detail is given regarding the expected responsibilities of that Accountable Executive. Note the accountable executive's span of control is expected to be very broad. The accountable executive is an individual whose roles and responsibilities include: establishing, implementing and maintaining the SMS. This is contrasted with the terms "Top Management" which can be a person or a group of people.

If the organization implementing SMS is a small business, it is possible that the accountable executive and "Top Management" are one and the same. [Part 5.25(a)]

1.3(2) – *This Sub-Element outlines in broad terms the tasks an accountable executive must accomplish. Most of the tasks are self-explanatory. The "substandard safety performance" referenced in Sub-Element 1.3(2)(e) is relative to the organization's own chosen goals and objectives.* [*Part 5.25(b)]*

The output of this expectation is expected to be a document that includes roles and responsibilities of the accountable executive.

1.3(3) – *The FAA recognizes that the details of establishing, implementing and maintaining an SMS and associated processes and procedures need to be handled by someone other than the accountable executive. The first three "details" reflect the SMS components themselves, while the fourth is the ever important upwards communication and feedback to the accountable executive. (The downward communication from the accountable executive to the employees is captured by Component 4.0, Safety Promotion, under Communications and Awareness.) It is expected that this designated management representative would be a member of the organization's top management ranks. [Part 5.25(c)]*

The output of this expectation is expected to be in the form of documentation which includes the roles and responsibilities of the designated management representative. An organizational chart may also be a useful additional aid to clarify the structure and reporting lines for specific positions.

1.4 Emergency Preparedness and Response

(STANDARD)

The organization will develop and implement procedures as necessary that it will follow in the event of an accident and incident.

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.27]

In the context of SMS and aviation safety, the terms "accidents" and "incidents" as used here may involve the organization's products and articles, flight test department(s), or involvement/support to accident or incident investigations. A design organization, for example, may need only to be put on alert if an accident aircraft has the organization's approved modification installed. Thus, these procedures may be tailored depending on the organization's size, type of business, and the types of accidents and incidents that are possible given its type of business.

The organization should develop a set of coordinated response procedures that describe the duties and responsibilities assigned to each department as well as each participant. The response should include the protection of response participants from unnecessary risks.

When responding to an emergency, it is imperative for organizations to have in place a written Emergency Response Plan, which consists of workable procedures that allow an organization to respond to an accident or any other crisis that could adversely impact operations, in a logical and coordinated manner. Following this plan should provide consistent and timely information to those that need it and prevent duplication of work.

The first step in the development of this plan is to identify and assemble a team of key personnel, each of whom will have specific, pre-assigned responsibilities and duties should an accident, incident, or other unplanned event occur. Obviously, the size of the team should depend on the size of the organization and include all departments and facets.

Another important consideration is communication. Each member directly participating in the emergency response activity should have a reliable way of communicating with one another to ensure information is exchanged directly and rapidly.

An accident/incident can happen at any time and in any place, and the person receiving the news might not be part of the response team. Therefore, at a minimum, an organization should determine what information it needs to collect in the event that it receives word of an accident/incident. The organization should also ensure employees are aware of the proper information to collect when learning of an accident or incident.

In executing an Emergency Response Plan, participants should actively look for, identify, and communicate the existence of unsafe conditions that they believe may

have contributed to the event. This enables the organization to search for any systemic safety errors and implement root cause solutions while the symptomatic cause is being investigated.

The best test of effectiveness of the Emergency Response Plan is to create periodic hypothetical accidents, incidents, or other catastrophic events. The organization should conduct periodic exercises of its response process to assure effectiveness and efficiency.

Additionally, an organization should have a process to deal with the results of environmental disasters or catastrophes with respect to their impact on the products, articles, or processes. For instance, a manufacturing organization that experiences a hurricane at one of its facilities should evaluate, among other things, damage to the products/raw materials, the equipment residing in the facility, and all other items supportive of the manufacturing process (including documentation, shop floor design, etc.). *[Part 5.27]*

1.5 SMS Documents and Records

(STANDARD)

The organization will develop and maintain documentation that describes the organization's safety policy and SMS processes and procedures.

The organization will:

(1) Maintain records of outputs of SRM and SA processes for as long as the affected aircraft, engine, propeller, or article remains in service;

(2) Maintain records of all training provided and a list of trained individuals, as required under Sub-Element 4.1.2, for a minimum of 24 consecutive calendar months after training completion;

(3) Retain records of all safety information communication for a minimum of 24 consecutive calendar months.

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.97]

1.5 – *The organization should document policies, objectives, procedures, and other related documents (i.e., detailed work instructions, forms, etc.) to ensure it can function in a standardized and consistent manner. A record may be proof that the organization has met requirements stated in documented policies, objectives, procedures, and other related documents. Records provide the organization with sufficient historical data to conduct the required analyses and assessments when necessary. Records and documents may be physical or electronic.*

SMS procedures and processes are those used to support meeting the SMS requirements and safety objectives. All processes and procedures should have a clearly identified person with the responsibility and authority to manage the process. [Part 5.97]

Best practices for documentation include the following:

- *Developing and implementing a procedure to control all SMS documents. This procedure would include requirements for approval prior to use, periodic review, and revision.*
- *Requiring that relevant documents are available at points of use.*
- *Ensuring that obsolete documents are not used.*
- *Maintaining documentation in an orderly manner – making it readily identifiable (by title, form number, etc.), retrievable, legible, and include a revision log with date of revision.*
- *Identifying specific periods for documents to be retained.*

1.5(1) – *Outputs of SRM include risk assessments, implemented risk controls, etc. Outputs of SA processes include audits and evaluations. [Part 5.97]*

2. Safety Risk Management

2.1 Hazard Identification and System Analysis

(STANDARD)

(1) The SRM process will be applied to:

(a) Initial designs of systems, organizations, and/or products; and the operation and maintenance of these systems, organizations, and/or products;

(b) The development of D&M processes and procedures;

(c) New or recurring hazards that are identified in the SA functions (described in Element 3.1), including information collected during design, manufacturing, operation and maintenance, etc; and

(d) Planned changes to D&M processes, including product, component, or part design changes, maintenance and operation instructions, and assumptions when a design is developed.

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.51, 5.53]

2.1 – *While it is recognized that identification of every conceivable hazard is impractical, organizations are expected to exercise due diligence in identifying and controlling significant and reasonably foreseeable hazards related to their business operations. [5.51]*

2.1(1)(a) – *When an organization determines that a new or changed system, organization, and/or product is required, it triggers the required use of the SRM processes and procedures. The FAA does not intend for an organization to apply SRM processes to established systems and processes without a trigger occurring under the SA component. In addition, it is not the intent of this expectation to require the application of SRM processes and procedures to activities that are not related to aviation. As an example, SRM would not be necessary when changing accounting practices or administrative computer software.*

2.1(1)(b) – *The SRM process is meant to be used throughout the lifecycle of the organization's product or service; that is, for a part or product, from design conception through development and implementation and until disposal or retirement. As applied to an organizational system or unit, the term "lifecycle duration" would be comparable, beginning with the design of the organizational unit itself. For example, one should ask what hazards can a new organization identify by virtue of its interfaces? its processes? its inputs and outputs? In this case, an organization's 'retirement' could be due to a superseding organizational structure or*

simply obsolescence. The feedback loops from SA need to be applied throughout the full lifecycle of the organization's product or service.

2.1(1)(c) – *Recurring hazards require the organization to always re-evaluate its original analysis, question past assumptions, review the data, and relook at the associated chosen risk control. Different risk controls may be found to be necessary in order to affect the recurrence. The effectiveness of the new control will have to be evaluated: does the hazard now abate or is it even eliminated? This is indicative of the cyclic nature of the two elements, SRM and SA.*

2.1(1)(d) – *Planned changes, usually undertaken as product improvements, will always need to be evaluated to ensure current risks are not exacerbated and/or substitute risks are not introduced.*

2.1.1 System Description and Analysis

(STANDARD)

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

(1) A system description and analysis will be developed to the level of detail necessary to identify hazards and implement risk controls.

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.53]

2.1.1 – *The intent here is for the organization to examine how it conducts its business so that it can develop a detailed System Description. The System Description defines the scope and boundaries of the organization that apply to an SMS.*

The System Description defines the organization by a set of system segments that represent its business in a manner that enables the identification of safety hazards related to its operations, processes, products, structure, interfaces, and environment. In defining its business through the System Description, the organization may elect an approach that creates segments based upon:

(1) Divisions, departments, or other organizational components e.g., facility, geographic area, combination of location and function or product line;

(2) Functions e.g., design, engineering, manufacturing, assembly, maintenance, marketing, and finance;

(3) Product lines e.g., designs, electronics, machined parts, engines, subassemblies, components, aircraft or engine models; or

(4) Another segmentation approach that more effectively characterizes the organization.

The organization uses the system segments to conduct its System Analysis identification of safety hazards and to execute its Preliminary Gap Analysis, Detailed Gap Analysis, and Implementation Plan in the Gap Analysis Tool. After performing the Preliminary Gap Analysis, the organization may refine its segments for use in the Detailed Gap Analysis and Implementation Plan. [5.53]

2.1.1(1) – *To proactively manage risk, an organization must be able to identify hazards within the system it has created. In order to identify those hazards and assess the associated risk, an organization must develop a "System Description" and conduct a "System Analysis."*

For D&M companies, the System Description needs to be developed to the level of detail necessary to identify hazards in both the organization that produces the end product (e.g., human factors, equipment, procedures, training, and related

operational environment aspects) and the end product itself (e.g., aircraft, engine, component, article, design approval, etc.).

Once the System Description is identified, the organization will conduct a System Analysis. The System Analysis is the process of analyzing all aspects of the System Description for the purpose of identifying hazards.

When developing a System Description and performing a System Analysis, an organization should take into account other entities (i.e. contractors, vendors, and customers who provide/use products/services) with which it interacts. These other entities' systems may introduce their own hazards that must be taken into account.

The System Description and System Analysis are fundamental steps in preventing safety issues from arising and making safety improvements. An organization that thoroughly understands where hazards exist within its system is in a better position to design and manufacture safer products than one that does not.

2.1.2 Identify Hazards

(STANDARD)

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. *{Sentence moved to DG}*

(1) Hazards will be:

(a) Identified for the scope of the system, as defined in the system analysis

(b) {Paragraph removed - duplication}

(2) {Paragraph moved to DG}

(a) {Paragraph moved to DG}

(b) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.5, 5.53, 5.97]

2.1.2 – *A hazard is defined as a condition that could forseeably cause or contribute to an aircraft accident. It is sometimes termed "threat." The organization should identify hazards for both the products they produce and the processes conducted by the organization.*

Examples of hazards include:

- *Undetected change in a system or process;*
- *Incomplete process definition;*
- *A product that deviates from its design;*
- *An unplanned work stoppage*
- *Removing or reducing inspections in the Quality Assurance area;*
- *Too many engineering changes**;***
- *Moving a production line, in whole or in part, to another location or supplier;*
- *Out-of-position work being performed by others not as qualified or knowledgeable (for example, as a result of vacations or attrition of the skilled workers);*
- *Personnel with insufficient aircraft-specific knowledge to appropriately assess compliance;*
- *Breakdown in safety information flowing from one person or organization to another;*
- *Key personnel are unaware of an issue;*
- *An initiative, change, new process, or other activity intended to improve something produces, in addition to the improvement, an undesirable outcome.*

(That is, an undesirable outcome occurs that would not have otherwise happened before the change.). *[5.5, 5.53(b),(c)]*

2.1.2(1)(a) – *While it is recognized that identification of every conceivable hazard is impractical, organizations are expected to exercise due diligence in identifying and controlling significant and reasonably foreseeable hazards related to their operations.* *[5.53(a), 5.97(a)]*

2.1.2(1)(b) – *Hazards should be documented. The kinds of documentation that would be expected for hazards are risk assessment and risk analysis reports, risk or hazard abatement procedures, and/or a service difficulty event report, log or database.*

2.1.2(2)(b) **–** *Hazard information should be tracked and managed throughout the SRM process. The intent of "managed" here is to ensure that hazard information is provided to those in the organization that are affected by and have an effect on the hazard and its mitigation so that the information is periodically reviewed to ensure its accuracy and whether current mitigation strategies are still valid.*

2.2 Risk Assessment and Control

(STANDARD)

(1) *{Paragraph moved to DG}*

(2) The organization will develop a risk acceptance process:

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

1. *{Paragraph moved to DG}*
2. *{Paragraph moved to DG}*

(d) *{Paragraph removed - duplication}*

(e) *{Paragraph moved to DG}*

(3) The organization will establish feedback loops from assurance functions described in Component 3.0, to evaluate the effectiveness of safety risk controls.

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.55, 5.73]

2.2 – *Risk is the composite of predicted severity (how bad) and likelihood (how probable) of the potential effect of a hazard in its worst credible system state.*

2.2(1) – *Top management should ensure that the hazards that introduce the most significant safety risk are prioritized and resources are directed to reduce/mitigate their safety risk to an acceptable level. Their allocation of resources should reflect an alignment to reducing and/or mitigating any risk that those hazards pose. The "most significant safety risk" means an unacceptable risk in terms of severity and likelihood.*

2.2(2)(a) – *The organization should develop a risk acceptance process that includes both quantitative and qualitative risk analyses as appropriate. The effectiveness of risk controls can be shown with quantitative and qualitative risk analyses. The difference between quantitative and qualitative risk analyses is that quantitative analysis deals with numbers and data that can be measured while qualitative analysis deals with observations that cannot be directly measured. Conclusions made from qualitative analysis are based on experience and subject matter expertise. [5.55(b), 5.73(a)(3)]*

2.2(2)(b) – *The organization must develop a risk acceptance process that defines acceptable and unacceptable levels of safety risk. An organization should define its own levels of acceptable and unacceptable risk. The levels of risk can be defined in*

terms of quantitative thresholds or via a qualitative risk matrix (with the two axes being "severity" and "likelihood"). However the organization defines its levels of risk, it must comply with applicable regulation.

It is important to note that the difference between acceptable and unacceptable levels of risk depends on the severity and likelihood of the potential effect of a hazard in its worst credible system state. A risk that has high severity but very low likelihood may be acceptable, while one with less severity but high likelihood may be unacceptable.

2.2(2)(c) – *The organization should develop a risk acceptance process that describes severity levels and likelihood levels.*

2.2(2)(d) – *The organization should develop a risk acceptance process that assigns specific levels of management that can make safety risk acceptance decisions. Actions taken to satisfy 2.2(2)(d) are to carry out the policy established under 1.2(4). An organization will determine which level(s) of management is responsible for accepting risk. The organization may choose to differentiate which level of management is responsible for specific levels of risk acceptance. For example, the highest level of risk acceptance may require senior management approval. The lowest level of risk acceptance may be performed by first line management.*

2.2(2)(e) – *The organization should develop a risk acceptance process that defines acceptable risk for hazards that will exist in the short-term while safety risk control/mitigation plans are developed and implemented. The intent of "acceptable risk for hazards that will exist in the short-term" is to determine via analysis (ideally quantitative risk analysis) that the risk exposure is small enough to remain uncorrected while a control or mitigation program is being developed.*

2.2(3) – *Examples of how an organization could evaluate the effectiveness of risk controls include test and analysis, and/or a service evaluation program. Additionally, an organization may collect service and operational event data as part of the SA function to determine if a risk control is adequately managing the risk and the safety issue (or potential safety issue) is no longer posing a threat. The individuals who identify risk controls should be involved in the determination of which data to collect and evaluate to determine the effectiveness of the risk control.*

A process that incorporates a safety assurance to safety risk management feedback loop will demonstrate that the processes are integrated and the expectation is met.

2.2.1 Analyze Safety Risk

(STANDARD)

The organization will determine and analyze the severity and likelihood of potential consequences associated with identified hazards and it will identify contributing factors.

(1) *{Paragraph moved to DG}.*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

1. *{Paragraph moved to DG}*
2. *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.55]

2.2.1 – *"Potential consequences" are those possible outcomes associated with a hazard while "contributing factors" are the actual causes of the hazard. Examples could be:*

Example 1
Contributing Factor(s): Incorrect work instructions
Hazard: Improperly fastened fuel line
Potential Consequence(s): Engine fire

Example 2
Contributing Factor(s): Improper material processing
Hazard: Material inclusion
Potential Consequence(s): Disk burst

A single hazard may have multiple potential consequences that may contribute to the resulting safety risk. Therefore, it is important that an organization identify all likely consequences that pose a safety risk and not just the obvious outcomes.

2.2.1(1)(a – c) – *The safety risk analysis process will include documenting the risk analysis results for each hazard, the analysis of existing safety risk controls, identification and analysis of contributing factors, and determination of safety risk of outcomes from the existence of a hazard, to include estimation of the likelihood, and severity. The process used to analyze the hazards should consider all the system segments.*
2.2.1(1)(d) – *The organization's safety risk analysis process should include existing safety risk controls, triggering mechanisms, and the safety risk of reasonably likely outcomes from the existence of a hazard. This process should include a*

determination of the risk's likelihood and severity, using quantitative methods whenever possible.

Other notes regarding Risk Analysis:

- *Implementation of new or changed system designs (including new or changed organizational elements or procedures) should not occur until the safety risk of each identified hazard is determined to be acceptable.*
- *Likelihood and severity may be expressed in quantitative or qualitative terms. However, it is best practice to use quantitative methods wherever possible. If it is not possible to use quantitative methods, organizations typically begin with quantitative estimates based on qualitative judgment. This allows for an organization to migrate towards quantitative methods over time.*
- *Values are assigned to the likelihood and severity of risks associated with identified hazards in order to establish a quantifiable standard. This both increases the objectivity of the risk analysis and allows employees to prioritize those risks that are most urgent.*

2.2.2 Assess Safety Risk

(STANDARD)

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.

(1) Each hazard will be assessed for its safety risk acceptability. *{Sentence deleted - reference removed}*

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.55]

2.2.2 – *In the development of its risk assessment criteria, organizations are expected to develop risk acceptance procedures, including acceptance criteria and designation of authority and responsibility for risk management decision-making. The acceptability of a risk may be determined using a risk matrix, which quantifies severity and likelihood. The objective of risk management should always be to reduce risk to as low as practicable, regardless of whether the assessment shows that the risk can be accepted as is. This is a fundamental principle of continuous improvement. All identified risks that are judged to be unacceptable must be mitigated to an acceptable level. [5.55(b)]*

For additional information, see guidance under Element 2.2.

2.2.3 Control/Mitigate Safety Risk

(STANDARD)

The organization will design and implement a safety risk control for each identified hazard for which there is an unacceptable risk, to reduce risk to acceptable levels.

(1) *{Paragraph Removed – Duplication}*

(2) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(3) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.55]

2.2.3 – *Safety risk controls should include a method to prioritize, track, implement, and determine the effectiveness of all actions taken.*

Safety risk controls are intended to improve the level of safety in the organization by lowering the risk associated with hazards that are identified in the organization's operation.

An example of an SMS output that can identify that this expectation has been met is: **Risk control or mitigation process or procedure document**.

The process or procedure could be included within a single composite document covering the entire safety risk management process or it may be comprised of individual procedures associated with each hazard identified. [5.55(c)(1)]

2.2.3(1) – *Safety risk control/mitigation plans must be defined for each hazard with unacceptable risk.*

2.2.3(2) – *Safety risk controls should be clearly described, capable of performing appropriately in the intended operational environment, designed to evaluate if the risk control expectations have been met and documented "Intended operational environment" is meant to place bounds on what can reasonably be expected for the safety risk control to be effective.*

2.2.3(3) – *"Substitute risk" is a risk that is unintentionally created as a consequence of a safety risk control. Substitute risk must also be analyzed and assessed and controlled when warranted.*

It is essential that all controls and mitigations be reviewed after implementation to assure they were fully implemented and are determined to be effective.

3. Safety Assurance

3.1 Safety Performance Monitoring and Measurement

(STANDARD)

(1) The organization will monitor its systems and operations to:

(a) Identify new and recurring hazards,

(b) Measure the effectiveness of safety risk controls,

(c) Ensure compliance with regulatory requirements.

(2) The organization will collect the data necessary to demonstrate the effectiveness of its systems and operations.

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71, 5.73]

3.1 – *The purpose of performance monitoring and measurement is to gain confidence in the performance and effectiveness of risk controls and to identify new hazards in the operational environment. More specific information is contained in the Sub-Elements that follow.* *[5.71(a), 5.73(a)]*

3.1.1 Continuous Monitoring

(STANDARD)

The organization will monitor data throughout the lifecycle, including those associated with components and services that are received from suppliers and contractors, to identify hazards, measure the effectiveness of safety risk controls, and assess system performance.

(1) {Paragraph removed – duplication}

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71, 5.73]

3.1.1 – *Changes in the operating environment and other sources can induce new hazards that the system has not previously experienced. Only through continuous monitoring can the effects of these new hazards be identified.*

Data monitored throughout the lifecycle may include statistical process control data, hours and cycle times on products, heat treat lot information, manufacturing lot data, and material review board findings.

3.1.1(1) – *The organization should monitor various types of data including reports from the employee safety reporting and feedback system (specified in Sub-Element 3.1.5) to:*

(a) Determine conformity to safety risk controls (described in Sub-Element 2.2.3);

(b) Measure the effectiveness of safety risk controls (described in Sub-Element 2.2.3);

(c) Assess SMS system performance; and

(d) Identify hazards.

Moreover, any data generated, gathered, stored, or supplied by external entities (e.g., consultants, contractors, vendors, customers, etc.) should also be monitored.

3.1.1(1)(a) – *"Conformity to safety risk controls" means that the controls are in place and being utilized correctly.*

*In Sub-Element 2.1.2 of the Developmental Guidance, examples of hazards are identified. Below are examples of the **possible** indicators that can be used during continuous monitoring to determine if hazards are coming to fruition:*

- *Hazard: Removing or reducing inspections in the Quality Assurance area; Indicator: New unforeseen problems/hazards.*
- *Hazard: Too many engineering changes;*

Indicators: Disrupted work flow, engineering errors or variances that end up driving an increase, rather than a decrease, in part defects.

- *Hazard: Moving a production line, in whole or in part, to another location or supplier;*
  Indicators: Part defects rise.
- *Hazard: Out-of-position work being performed by others not as qualified or knowledgeable (for example, as a result of vacations or attrition of the skilled workers);*
  Indicators: Errors in work performed; slowed production.
- *Hazard: Personnel with insufficient aircraft-specific knowledge to appropriately assess compliance;*
  Indicator: Compliance absent or incomplete; repetition of documentation review.
- *Hazard: Breakdown in safety information flowing from one person or organization to another;*
  Indicators: The information shared is incomplete or inaccurate; needed historical information is lost.
- *Hazard: Key personnel are unaware of an issue;*
  Indicators: Rising number of part defects; multiple review cycles for the same issue
- *Hazard: An initiative, change, new process, or other activity intended to improve something produces, in addition to the improvement, an undesirable outcome. (That is, an undesirable outcome occurs that would not have otherwise happened before the change.)*
  Indicator: Information was 'forgotten' that, if remembered, could have been used to prevent the undesirable outcome.

3.1.2 Internal Audit

(STANDARD)

The organization will conduct internal audits of the SMS to determine if the SMS conforms to the organization's processes and procedures.

(1) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(2) *{Paragraph moved to DG}*

(3) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71]

3.1.2 – *The purpose of the internal audit is for the organization to determine whether it is conforming to its SMS. The question to ask and answer is, "Is the organization conforming to its processes and procedures?"*

3.1.2(1)(a-b) – *The audit should be conducted to account for:*

(a) Safety criticality of the systems and operations being audited, and

(b) Results of previous internal and external audits.

Procedures should be established that include responsibilities and requirements for planning and conducting audits. These procedures also should include reporting requirements and a means of analyzing the results. Vendors and contractors should be included in the audit plan.

It is essential to audit an organization's activities to determine if its employees and business units follow the processes and procedures as they were designed.

3.1.2(2) – *The scope of the internal audit program should cover the entire organization's SMS within a specified timeframe. During its audit planning, an organization should include definitions of its audit criteria, scope, frequency, and methods. Audit records should be maintained. An organization may find it practical to expand its current internal audit program to include the safety expectations of their SMS.*

3.1.2(3) – *The organization should include in its analysis of data, the results of assessments performed by oversight organizations. [5.71(a)(1-4)]*

3.1.3 Internal Evaluation

(STANDARD)

The organization will perform regularly scheduled internal evaluations of its systems and operations to determine the performance and effectiveness of risk controls.

(1) *{Paragraph moved to DG}*

(2) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71]

3.1.3 – *The purpose of the internal evaluation is for the organization to determine whether its SMS is performing as intended and achieving the organization's safety objectives. The question to ask and answer is, "Is the organization meeting its own expectations for safety?" The evaluation should also be used to identify where improvements can be made to the SMS.*

During its evaluation planning, an organization should include definitions of its evaluation criteria, scope, frequency, and methods.

It is essential to evaluate an organization's processes to ensure that they are effective and provide the intended results for which they were designed.

3.1.3(1) – *Procedures should be established that include responsibilities and requirements for planning and conducting evaluations. The entire scope of the organization's SMS as defined by the system definition (expectation defined in Sub-Element 2.1.1) should be included in the evaluation. These procedures should also include reporting requirements and a means of analyzing the results.*

3.1.3(2) – *Vendors, suppliers and contractors of safety-related functions should be included in the evaluation plan. Records of evaluation results should be maintained.*

It is essential to evaluate an organization's processes to ensure that they are effective and provide the intended results for which they were designed. [5.71(a)(1-4)]

3.1.4 Investigation

(STANDARD)

The organization will establish procedures to collect data to investigate instances of potential regulatory noncompliance and to identify potential new hazards or risk control failures.

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71, 5.73]

3.1.4 – *The progress of safety management through its history has always been dependent on the results of accident investigation to make operational system improvements. Previously, the approach to safety management was based solely on accident investigation and regulatory compliance. These techniques must still be used **as part of** a comprehensive program for managing risk. The goal of safety management systems today is to attain higher levels of safety by proactively identifying and managing risk.*

The types of investigation intended by this expectation include both reactive and proactive investigation. For example, one type of proactive investigation would be to determine the hazards causing negative trends in manufacturing tolerances before limits are exceeded.

"Potential regulatory noncompliance" means that a regulatory noncompliance has not yet occurred. However, there is some shift or trend evident such that if preventive action isn't taken, a noncompliance is expected to eventually occur. This should initiate an investigation into the cause and subsequent remedy.

3.1.5 Employee Reporting and Feedback System

(STANDARD)

The organization will actively use an employee safety reporting and feedback system.

(1) *{Paragraph moved to DG}*

(2) Employees will be encouraged to submit solutions/safety improvements.

(3) *{Paragraph moved to DG}*

(4) *{Paragraph moved to DG}*

(5) Employees will be allowed confidentiality when using the employee safety reporting and feedback system.

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71]

3.1.5 – *The term "actively" used here is meant to imply that employees and management are using the system and it is not merely in place to meet the expectation. Additionally, the system needs to be available full-time (when employees can use it).*

3.1.5(1) – *Data obtained from the employee reporting and feedback system should be monitored to identify emerging hazards and to assess performance of risk controls in the operational systems. The employee reporting and feedback system should produce tangible actions and outcomes.*

3.1.5(2) – *Often the best source of information concerning the problems in organizations is the employees that work closest to the process. As with any quality improvement method, safety management systems require information that only the employees possess concerning the true effectiveness or brittleness of the system. Employees are most often the best source for solutions to operational problems. To make employees more comfortable in providing such information, an organization's reporting system should be non-punitive. This policy would not apply to illegal acts or a willful disregard of regulations or procedures.*

3.1.5(3) – *Data collected from the safety reporting and feedback system should be included in analyses described in Sub-Element 3.1.6.*

3.1.5(4) – *For the employee reporting and feedback system to be effective the employees must feel that they are being heard. For this reason, management should respond to all submissions with rationale for their chosen action or inaction. For efficiency, management may choose to post responses to a website or publish responses in newsletters rather than sending individual responses to each submitter.*

This approach is especially useful when responding to numerous similar submissions and anonymous submissions.

The organization should adopt an open-door policy where employees feel free to discuss issues openly with each other and management. It is important, however, that when a comment or suggestion is made informally there be some mechanism to document it formally. [5.71(a)(7)]

3.1.6 Analysis of Data

(STANDARD)

The organization will analyze the data acquired in Sub-Elements 3.1.1 through 3.1.5 to assess the performance and effectiveness of risk controls in the organization's systems and operations.

(1) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.71]

3.1.6 – *An organization's data analysis should include data from the Employee Reporting and Feedback System (3.1.5), information related to customer satisfaction, including customer feedback and customer complaints as well as the results of continuous monitoring of operational data, auditing, and investigations. All information available should be collected and included in the data analysis.*

3.1.6(1)(a-d) – *The organization should analyze the data described in Sub-Elements 3.1.1 through 3.1.5 to:*

(a) Assess the effectiveness of risk controls,

(b) Identify where current risk controls are deficient,

(c) Identify potential new hazards which need risk control, and

(d) Identify where improvements can be made to the organization's risk controls.

Anything identified to have a safety implication should be subject to a System Assessment (3.1.7) to determine if new hazards, and therefore requirements for SRM, exist. [5.71(b)]

3.1.7 System Assessment

(STANDARD)

The organization will assess the safety performance and effectiveness of risk controls, its ability to achieve the organization's safety objectives, and its conformity to the design of the organization's SMS.

(1) The organization will assess the performance of:

(a) Risk controls put in place by the organization for their effectiveness,

(b) Safety-related functions of the design and production-related processes against its objectives and expectations,

(c) The SMS against its objectives and expectations.

(2) The organization will use the information obtained under Sub-Element 3.1.6, and from other sources as necessary, to make its assessments.

(3) System assessments will document results that indicate a finding of:

(a) Conformity with existing safety risk control(s)/the organization's SMS expectations(s) (including regulatory requirements applicable to the SMS);

(b) Nonconformity with existing safety risk control(s)/the organization's SMS expectations(s) (including regulatory requirements applicable to the SMS); and

(c) New hazards found and how the organization will deal with them.

(4) *{Paragraph moved to DG}*

(5) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

1. *{Paragraph moved to DG}*
2. *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

1. *{Paragraph moved to DG}*
2. *{Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(6) The SRM process will be utilized if the analysis of data from Sub-Element 3.1.6 indicates:

(a) The identification of new or potential hazards, or

(b) The need for system changes.

(7) *{Paragraph removed – duplication}*

(DEVELOPMENTAL GUIDANCE)

[Corresponding Part 5 NPRM reference: 5.73]

3.1.7 – *The organization will assess the safety performance and effectiveness of risk controls and conformance to this Framework's expectation(s). System Assessment is the decision function that follows Data Analysis and determines whether further risk analysis is required or what corrective action should be taken. This process of creating effective methods to manage identified risks can reduce or eliminate the potential for accidents and other unwanted events.*

3.1.7(5) – *The organization should develop safety lessons learned to support continuous improvement of safety.*

3.1.7(5)(a) – *The organization should develop:*

(1) Corrective actions for identified nonconformities with risk controls, and

(2) Preventive actions for identified potential nonconformities with risk controls.

While the need for corrective action may be obvious, identifying potential nonconformities may be more difficult. To accomplish this, an organization may need more sophisticated or robust techniques or methods to notice such adverse trending or imminent risk.

System assessments should result in the documentation of the near or actual nonconformity with existing safety risk control(s) and/or SMS expectation(s).

3.1.7(5)(b) – *In the process of developing corrective and preventive actions, the organization should take into account safety lessons learned in addition to typical factors, such as: time necessary to implement the action, facilities and equipment necessary/available to take the action, skills required to implement the action, complexity of the action, etc.*

3.1.7(5)(c) – *When prioritizing and implementing corrective and preventive action(s), the organization should give priority to those that address the greatest safety risk.*

3.1.7(5)(d) – *Records of the disposition and status of corrective and preventive actions, as well as other safety assessments, should be maintained, as required per Element 1.5. [5.73(a)(1-2)]*

3.1.8 Management Review

(STANDARD)

As part of their commitment to continual improvement, top management will conduct annual reviews of the SMS, at a minimum. Management reviews will include assessing the performance and effectiveness of the organization's systems and operations and the need for improvements.

(1) *{Paragraph moved to DG}*

(a) *{Paragraph move to DG)*

(b) *Paragraph moved to DG}*

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(2) *{Paragraph moved to DG}*

(3) *{Paragraph moved to DG}*

(4) *{Paragraph removed due to duplication}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding Part 5 NPRM reference: 5.73, 5.75]

3.1.8 – *Management reviews of all aspects of SMS performance is necessary to close the feedback loop back to the original Safety Plan (reference Element 1.1(5)). The management reviews must be conducted at a minimum of one per year. This review may be chosen to coincide with other Internal Audits or Evaluations. The outputs reviewed should include those from:*

(a) The outputs of safety policy (Component 1.0);

(b) The outputs of SRM (Component 2.0);

(c) The outputs of SA (Component 3.0);

(d) The outputs of safety promotion (Component 4.0).

3.1.8(2) – *Top management reviews should include assessing the need for improvements to the organization's SMS. Top management should retain and use this information to improve the organization's SMS by modifying the Safety Management Plan as necessary. The Management Review process is crucial in demonstrating management commitment and ensuring the effectiveness of the SMS.*

3.1.8(3) – *Top management should document, distribute, and review the findings and inform their employees of the ensuing actions, as appropriate. It is important for all employees to understand the changes to the organization's system and why they occurred.*

3.1.8(4) – *Top management should maintain records of the reviews and their findings in accordance with Element 1.5.* *[5.73(a-b), 5.75]*

3.2 Management of Change

(STANDARD)

The organization will identify and assess safety risk for changes arising within, or external to, the organization that may affect established systems or operations. These changes may be to existing system designs, new system designs, or new/modified operations or procedures.

(1) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(2) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding NPRM Part 5 reference: 5.53 – 5.75]

3.2(1) – *The organization should not implement changes until the safety risk of each identified hazard is determined to be acceptable. Changes external to the organization (e.g., moving to new manufacturing sites (especially out of country), etc.) can create hazards.*

3.2(1)(a-b) – *The organization should identify hazards and assess safety risk of the following before implementation:*

(a) New or changed system designs, and
(b) New/modified operations or procedures.

System designs identified above in Section (1)(a) are meant to include, but not be limited to:

- *Aircraft, engines, propellers, components, parts, articles, etc.;*
- *SMS processes and procedures;*
- *Operational processes and procedures;*
- *A company's organizational structure.*

3.2(2) – *If a system, process, or procedure requires urgent change, the organization may take interim immediate action(s) to mitigate existing safety risk prior to completing the full "Management of Changes" process. It is recognized that there are certain urgent circumstances where a full evaluation under the Management of Change process would not be completed quickly enough to address imminent risk. In these cases, the organization may take an "interim immediate action" to lower the safety risk until a full Management of Change process is completed. Once the full process is completed, a more comprehensive risk mitigating action may be identified and implemented.*

In general then, the organization needs to design their "Management of Change" process to be robust enough to account for the different sets of circumstances that are frequently encountered: those pertaining to urgent need for change, routine day-to-day design changes, and all other change circumstances in-between. [5.53-5.75]

4. Safety Promotion

4.1 Competencies and Training

4.1.1 Personnel Expectations (Competence)

(STANDARD)

The organization will document SMS competency requirements for those positions identified in Elements 1.2(3) and 1.3 and ensure those requirements are met.

(1) {Paragraph moved to DG}

(2) {Paragraph moved to DG}

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.91]

4.1.1 – *The organization must develop a minimum qualification standard for safety-related personnel and ensure those individuals meet or exceed that standard. By ensuring the appropriate personnel are competent, an organization will reduce the risk of error in the performance of its safety-related functions. [Part 5.91]*

4.1.1(1-2) –

(1) The organization must determine and document SMS competency requirements for those positions identified in Elements 1.2(3) and 1.3.

(2) The organization must ensure that those individuals in the positions identified in Elements 1.2(3) and 1.3, meet the Sub-Element 4.1.1(1) SMS competency requirements.

See the definition for "Competency" in the D&M SMS Pilot Project Guide. While competencies are knowledge, skills, and abilities obtained through education, training, and experience, SMS competencies refer only to those skills and abilities that are needed for personnel to perform their role within the organization's SMS. SMS competencies are needed by safety-related personnel and their management.

Some organizations may choose to use a Competency Requirements Matrix or Job Skills Analysis to make their determinations, which could satisfy this expectation. [Part 5.91]

4.1.2 Training

(STANDARD)

The organization will develop and maintain a safety training program that ensures personnel are trained and competent to perform their role within the SMS. The organization will also regularly evaluate training necessary to meet competency requirements of Sub-Element 4.1.1.

(1) *{Paragraph moved to DG}*

(2) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.91]

4.1.2 – *Training is essential to any corporate improvement effort and the SMS is no exception. The safety training program should be used to provide the common philosophy, direction, expectations, and procedural requirements necessary for the SMS to be effective.*

The safety training program often consists of initial and recurrent training components. Training can be conducted using different methods, which may extend beyond the usual formal classroom-based instruction (e.g. computer based training, newsletters, shift meetings, videos). Additionally, "recurrent" training doesn't necessarily require annual classroom-based events. Recurrent training should be provided as the need is apparent (e.g., weekly/monthly spread throughout a defined period, semi-annual, etc.). [Part 5.91]

4.1.2(1) – *Training should be developed and/or acquired and administered to employees, corresponding to their safety-related roles/responsibilities within the organization. Training should take into account the scope, content, and frequency needed to ensure competency is established and maintained.*

For each safety-related role/responsibility, the organization should define a SMS training standard that should remain current through periodic reviews and updates. The training standard should define annual (or other periodicity) training and testing requirements. If a job changes significantly, it may be necessary to update the training standard and provide additional training to select personnel. [Part 5.91]

Examples of training that match specific safety-related roles/responsibilities could be:

> ***Job**: Continued Operational Safety (COS) Engineer*
> ***Safety-Related Role/Responsibility**: COS and SA function*
> ***Typical Training Requirement**: Introduction to Root Cause Analysis (RCA), Introduction to Auditing Techniques.*
>
> ***Job**: Machinist*
> ***Safety-Related Role/Responsibility**: Hazard and Event Reporting*
> ***Typical Training Requirement**: Use of organization hazard reporting process and systems*

4.1.2(2) – *To ensure training currency, training should be periodically reviewed and updated. If it is deemed that training is not meeting the organization's needs, or changes have been made to processes, the organization should evaluate existing training and determine how training should be updated. [Part 5.91]*

> ***Example 1***
>
> **Situation**: *An organization currently has a manual (paper-based) risk analysis process. This organization procures a new, automated risk-analysis tool, which most of its personnel have never used.*
>
> **Action:** *The organization must identify updates that are necessary to its existing risk-analysis training to incorporate use of the tool. Additionally, the organization must identify how and when to deliver training to personnel who will now use the automated tool, but were previously trained on the manual risk analysis process.*
>
> ***Example 2***
>
> **Situation**: *An organization identifies a trend (via an annual performance/training review) that indicates multiple individuals appear to be deficient or not knowledgeable of the "Hazard and Event Reporting" process.*
>
> **Action**: *The organization must review the corresponding "Hazard and Event Reporting" process training to determine how it should be updated. The organization must then determine how the training should be delivered to ensure the appropriate level of competency is met.*

4.2 Communications and Awareness

(STANDARD)

{Opening paragraph moved to DG}

(1) Top management will communicate to the organization, at a minimum, the following information:

(a) Rationale behind decisions to implement controls, preventive actions, and corrective actions;

(b) Rationale behind decisions to not take action;

(c) *{Paragraph moved to DG}*

(d) *{Paragraph moved to DG}*

(2) Top management will make SMS information readily accessible to anyone in the organization that will use it corresponding to their safety-related role/responsibility(ies).

(3) The organization will provide the FAA ready access to the outputs of the SMS.

(4) *{Paragraph moved to DG}*

(5) *{Paragraph moved to DG}*

(6) *{Paragraph moved to DG}*

(a) *{Paragraph moved to DG}*

(b) *{Paragraph moved to DG}*

1. *{Paragraph moved to DG}*
2. *{Paragraph moved to DG}*
3. *{Paragraph moved to DG}*
4. *{Paragraph moved to DG}*
5. *{Paragraph moved to DG}*
6. *{Paragraph moved to DG}*

(DEVELOPMENTAL GUIDANCE)
[Corresponding cross reference to NPRM Part 5: 5.93]

4.2 – *Top management should communicate the outputs of its SMS to its employees, and provide the oversight authority access to SMS outputs in accordance with established agreements and disclosure programs.*

Top management should consider communicating the outputs of its SMS to its employees through the following: e-mails, postings throughout the facility, and/or an SMS website where information is available to all employees. The intent is that the chosen delivery method ensures broad dissemination and achieves employee awareness. Multiple delivery methods may be necessary; this choice is at the discretion of the organization. An example of "access" could include: username and password security authorization to a company-owned, web-based system containing SA audit results. [Part 5.93]

4.2(1)(a) & (b) – *It is important for employees to understand what decisions are made to enhance safety. This includes the decisions to not take action and the rationale behind the decisions, which reflect that the organization reviews all submissions and assesses whether or not to take action. This also presents a positive cultural aspect to employees – what they report matters. When an employee submits a safety concern (e.g. new hazard information, event, etc.), management makes it visible that they have considered the submission and provides rationale for why they may have chosen not to take action. This reinforces the point that the employee's input is not ignored.* *[Part 5.93]*

4.2.1(c) – *Rationale, importance, and definition of the organization's SMS objectives are important aspects of top management's communications. They are the words that underlie the subsequent actions top management takes in their fulfillment of safety promotion.*

4.2(1)(d) – *Information on safety lessons learned is valuable to the organization's growth and maturity.*

The organization should consider the sharing of lessons learned and the use of best practice a fundamental method in the development of a safety culture. This enables the organization to benefit from past mistakes (to avoid recurrence) and its successes when processes and procedures are well executed (to promote and advocate the repeat application). The lesson learned process is often linked to employee incentive schemes to encourage the development of continuous process improvement and best practice.

4.2(2) – *"Readily accessible" used in this expectation refers to the most appropriate means of providing information to employees. This can include emails, postings throughout the facility, and/or an SMS website where information is available to all employees.* *[Part 5.93]*

4.2(3) – *The organization must provide access of SMS outputs to the FAA; Safety critical information must be made readily accessible upon request to anyone who is involved in a particular issue that requires the information, including the FAA when reviewing the safety outputs. It is important that the FAA has the proper information to support further safety analysis related to the products, components, or parts that the company produces.*

Providing "ready access" is intended to mean that the company shares information in such a way that supports the FAA's ability to perform its safety mission efficiently. A company should not withhold information in such a way that impedes or delays the FAA's ability to perform its safety mission. *[Part 5.93]*

4.2(4) – *The organization's SMS should facilitate the sharing of information with other organizations to manage issues of mutual concern.*

One way to promote safety throughout the aviation community is to contribute to the collective knowledge of safety issues and mutual concerns. Therefore, it is imperative that organizations' SMS support the sharing of information with other

entities. However, it is understood that some information that organizations maintain is proprietary and may not be appropriate to share. [Part 5.93]

Best practices that enable the sharing of information include:

- *Establishing communications channels with other companies, industry partners, and the FAA;*
- *Creating a process to capture knowledge (lessons learned) of safety issues;*
- *Storing information (e.g. lessons learned, safety information, etc.) in such a manner as to make it available quickly and easily; and,*
- *Participating in aviation safety symposia and other forums.*

4.2(5) – *The organization should periodically survey employee acceptance of and involvement in the organization's SMS.*

Safety is everyone's job. All employees need to understand their part and role in assuring safety, especially the importance of raising safety concerns through the SMS. This can be evaluated by using employee surveys, questionnaires and the utilization of the employee reporting and feedback system. [Part 5.93]

In order to achieve success in the SMS implementation, the organization should determine the extent to which employees are aware, knowledgeable, and involved in SMS implementation. Implementing the SMS cannot be successful without the acceptance and involvement of the employees.

Example method(s) to track and evaluate:

1) ***Tracking**:*
    a. *Document meetings where employees are involved in SMS development (e.g., SMS training, safety risk board meetings)*
    b. *Collect information on use of employee feedback and reporting system*
    c. *Collect information from employees on whether they use the hazard information identified within SMS processes in their job*
2) ***Evaluating**:*
    a. *Analyze feedback collected during meetings where employees are involved – does there appear to be resistance?*
    b. *Analyze the amount of use of the employee feedback and reporting system – does it appear that employees are using it appropriately to report issues?*
    c. *Are employees using hazard information in their new design and innovation activities?*

The following actions by top management encourage employee engagement: communicating safety critical outputs of the SMS to the organization, including the rationale behind decisions to implement controls, preventive actions, corrective actions or their rationale behind decisions to not take immediate action; stressing the

importance of an SMS, the organization's safety objectives, and safety lessons learned; encouraging certain outputs be monitored for further information.

The organization that tracks and evaluates employee involvement in SMS development, implementation and promotion will help ensure its own success by building mutual trust within the organization and promoting a positive safety culture.

4.2(6) – *Top management should promote the growth of a positive safety culture.*

Organizations with a positive safety culture are characterized by communication founded on mutual trust. Truth in communication is the foundation upon which trust is built. Organizations with the most positive safety cultures will, by definition, have open attitudes toward safety, which will be reflected in the free exchange of safety information both internally and externally, with oversight authorities and industry partners. [Part 5.93]

4.2(6)(a) – *Top management should publicize their stated commitment to safety to all employees.*

"Publication" is not intended to mean only the traditional form of publication via a letter, poster, or other physical media. Publication can be accomplished via: email, website, or other electronic means.

Top management's stated commitment to safety, safety responsibilities, safety policy, goals, objectives, standards, and performance will be available in areas defined for communication information as well as through e-mail notification.

4.2(6)(b) – *Top management should demonstrate their commitment to the SMS by:*

4.2(6)(b)*1* – *Communicating safety policy, goals, objectives, standards, performance and the safety responsibilities for the organization's personnel to all employees.*

*Top management should ensure that employees understand who is responsible for safety in the organization and what the key safety personnel are responsible for. Additionally, top management should ensure that employees understand that safety is **everyone's** responsibility. It is not expected that top management communicate each and every employee's safety responsibilities to all employees.*

4.2(6)(b)*2* – *Creating or providing access to an effective employee reporting and feedback system that provides confidentiality.*

An "effective" employee reporting and feedback system is one where the entire organization has been informed of its existence, trained in its use, and encouraged by management to participate in reporting. Members of the organization not only report errors made, but also proactively report hazards that may potentially result in dangerous conditions for them or others in the organization. All reports are tracked to determine the frequency of occurrence for the reported situation and are analyzed to determine the depth of further study needed to properly assess the associated risk. Feedback is given to the organization on the decision to implement risk controls and when no action is deemed necessary.

"Providing the option for confidentiality" allows an employee to ask for confidentiality when reporting through the system. This is frequently needed to protect an employee when s/he is reporting information that affects a superior or another person in the company that could impact the employee's job. Additionally, offering confidentiality can also influence an employee to report more information than they would otherwise feel comfortable doing.

4.2(6)(b)*3* *– Using a safety information system that provides an accessible, efficient means to retrieve safety information.*

A "safety information system" can be as simple as a journal or as complex as a web-based data storage/retrieval system. The form it takes on is less important than its accessibility to the workforce.

"Accessible" and "efficient" are important aspects to any system that is used to store and retrieve safety information. The more accessible and easy-to-use a system is, the more it will be used. When implementing a safety information system, a company should avoid making it burdensome to store and retrieve information from the system (e.g., only a few employees have access to the system, bureaucratic processes make it difficult to acquire access permissions, etc.).

4.2(6)(b)*4* *– Managing the risk-based, data-driven decision making processes.*

Top management should demonstrate a commitment to risk-based, data-driven decision-making by being involved in the processes and using risk information and data to make decisions.

Safety is everyone's responsibility. All employees should understand their role in assuring safety, especially the importance of raising safety concerns through the SMS.

The organization should provide access to the outputs of the SMS to its oversight organization, in accordance with established agreements and disclosure programs. When information is being disseminated a de-identification system should be used to maintain confidentiality.

Unless it is demonstrated that the organization learns from its failings, it will never reduce its risk. When it is apparent that the organization does this, its safety message becomes credible to the employees whose participation is essential to the success of the SMS.