
# SMS

# Guidance

# Manual

**Third Edition January 1, 2012**

**International Business Aviation Council (IBAC)**
**Suite 16.33, 999 University Street**
**Montreal, Quebec, H3C 5J9, Canada**

***www.ibac.org***

# Table of Contents

# 1. INTRODUCTION

Safety management systems are an evolutionary development of the traditional flight safety program that can significantly enhance the safety of an aviation operation. A successfully developed and implemented safety management system, or SMS, will ensure that safety is a core value in an organization or flight operation and that safety is integrated into all management systems including operational, maintenance, financial and human resource management.

This manual has been developed to assist aircraft operators develop and implement an effective safety management system that is appropriate to the size and complexity of their operation. The material contained in the manual is designed to provide an understanding of safety, safety management concepts and how safety management systems can be applied in a business aviation flight department or similar small commercial operation. The manual also provides information on the processes and procedures involved in SMS development, implementation and maturation, and how an SMS can be used to enhance the safety, efficiency and effectiveness of an organization or flight operation.

IBAC would like to acknowledge the many operators, organizations and individuals that contributed material that was used in the in the development of the manual and that participated in its development. Your generosity and dedication to the enhancement of aviation safety is very much appreciated.

# 2. INTRODUCTION TO SMS

## 2.1 Definition of Safety

The "meaning" of safety depends on one's perspective and the context of the activity. While safety can be considered as "zero risk of accidents", it is understood by everyone involved in aviation that the risk of accidents is always present.

Consequently, it is more appropriate to consider safety as:

**Safety**

*The state in which the risk to harm to persons or damage to property is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.*

This is the definition of safety that will be used throughout this document.

## 2.2 IS-BAO SMS Definition

Next it is important to ensure an understanding of what a safety management system is. The definition used in the *IS-BAO an International Standard for Business Aircraft Operations* is that a safety management system is:

**SMS – IS-BAO**

*The systematic and comprehensive process for the proactive management of safety-risks that integrates the management of operations and technical systems with financial and human resource management.*

This definition stresses the **systematic** nature of an SMS. A system can be viewed as a group of processes that act together to transform inputs into a desired output. A system usually has a clear purpose or objective and a process or a set of processes, to achieve the objective, plus a means of measuring the degree to which the objective has been achieved.

The definition also stresses that an SMS is a **comprehensive process**. That is that it is not just a "pilot thing" or "maintenance thing", but it includes all aspects of the operation.

The purpose of an SMS is the **proactive management of safety-risks.** This reinforces the concept that an SMS must be looking forward, not focused on history. The definition also notes that an SMS must not be considered as a stand-alone system related to any one part of the operation, but that it must integrate all of the systems used to **manage operations, maintenance, finance and human resources.**

## 2.3 ICAO SMS Definition

The International Civil Aviation Organization uses a slightly more simple definition of a safety management system. In their documentation they define an SMS as:

**SMS - ICAO**

*A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.*

The ICAO definition stresses the structural aspects of an SMS. However, if the ICAO and IS-BAO definitions are carefully considered, it is readily apparent that they are not in conflict but are, in fact, complementary

## 2.4 Functional Definition

Functionally an SMS can be described as a system where the hazards and the associated risks that are inherent in a flight department or company's operation are identified and analyzed. Action is then taken to either eliminate the hazards or to manage the related risks to a level as low as reasonably practicable by reducing the likelihood of an occurrence or its severity should there be an occurrence.

The next step is then to track those actions taken to manage the risks (mitigation) to verify that they are appropriate and effective. At the same time the processes are employed to identify new and emerging hazards or any that were missed in the original hazard identification. An SMS also includes to processes to monitor and measure safety performance and to evaluate the results of the safety management activities.

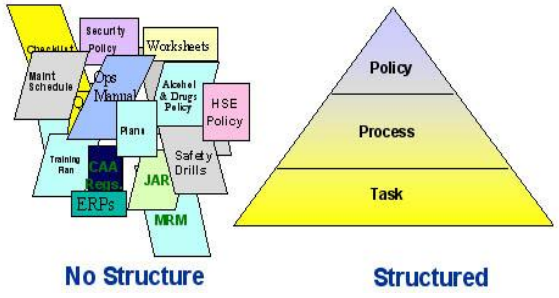
- Identify hazards.
- Analyze associated risks.
- Eliminate hazards (when possible), or
- Manage risks to a level as low as reasonably practicable (by reducing their likelihood or severity).
- Track to verify mitigation is appropriate and effective.
- Employ processes to identify additional hazards
- Monitor measure and evaluate safety performance

All of this is done within a clearly defined framework of safety objectives, polices, procedures and accountabilities.

- Safety objectives
- Polices
- Procedures
- Accountabilities

## 2.5 Safety Management System

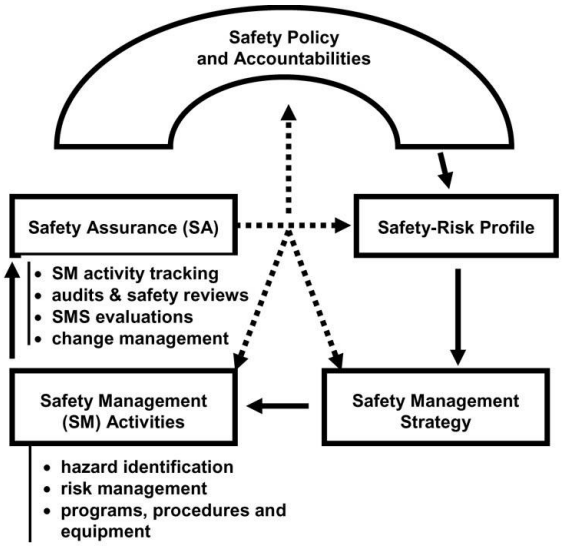
What we want to achieve with a safety management system is to put the proven safety management process together in a sound framework so that the processes work as a system to enhance the safety, efficiency and effectiveness of the operation. We want to systematically and proactively anticipate the hazards, and thereby take the "surprises" out of managing aviation by making appropriate and effective risk management decisions.




In a safety management system the safety policy, procedures and accountabilities are the umbrella under which the safety management system operates.

Under that "umbrella" the hazards and associated risks inherent in the operation are identified and assessed and a Safety Risk Profile is developed. The mitigation developed, to either eliminate the hazards or reduce the associated risk to a level as low as reasonably practicable and the safety goals for the operation are the foundation of the Safety Management Strategy. This Strategy is then implemented through programs, procedures equipment and training as appropriate. These are the Safety Management Activities. Safety assurance activities including the feedback from tracking the appropriateness and effectiveness of safety management activities, through the identification of additional hazards and the results of audits, safety reviews and SMS evaluations, all provide the information that is analyzed and used to adjust the Safety Risk Profile, Safety Management Strategy and Safety Management Activities as indicated by the dotted lines in this graphic depiction of a safety management system.

**Safety Management System**




ICAO has described a safety management system as being composed of four components with 12 elements. They are as follows:

**1. Safety Policy and Objectives**

1.1 Management commitment and responsibility

1.2 Safety accountabilities

1.3 Appointment of key safety personnel

1.4 Coordination of emergency response planning

1.5 SMS documentation

**2. Safety Risk Management**

2.1 Hazard identification

2.2 Safety risk assessment and mitigation

**3. Safety Assurance**

3.1 Safety performance monitoring and measurement

3.2 The management of change

3.3 Continuous improvement of the SMS

**4. Safety Promotion**

4.1 Training and education

4.2 Safety communication

While this may be a slightly different presentation, the end result and the means to achieve these elements are the same. More details of the components and their elements are contained in Appendix A.

Also of interest may be the FAA SMS Advisory Circular number 120-92A at: http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/0/678110F11B8433728625777D0068D732?OpenDocument&Highlight=120-92a , the FAA SMS guides posted on the IBAC web site at http://www.ibac.org/safety-management/sms-information-library and the Transport Canada SMS information at: http://www.tc.gc.ca/eng/civilaviation/standards/sms-menu-618.htm. Additionally, the Safety Management International Collaboration Group paper discusses some key aspects of an SMS.

It is important to understand that safety management systems are not stand-alone processes but are really part of an effective management system for any operation. As such, the safety management system must be compatible with other management systems and where possible, integrated with them.

It is also essential that the SMS be appropriate to the nature, size and complexity of the operation and the hazards and associated risks that are inherent in its activities. The SMS also must be periodically evaluated to verify that it remains effective.

**SMS must be:**

- consistent with the nature of and integrated into other management systems, and
- appropriate to the size and complexity of the operation.

Consequently, the safety management system used by an owner operator of a single aircraft, or a one-aircraft flight department, should be simpler and much less complex than the safety management system of a large, multi-aircraft corporate flight department or an on-demand charter operation.

## 2.6 Potential Results

Safety management systems have been effectively implemented by operations that range from those involving a single aircraft operated by the owner, to large international air transport operations.

Operators who have developed and implemented appropriate and effective safety management systems report that they have an extremely positive impact on their operation. Many have identified financial benefits that more than offset the costs associated with their SMS – in addition to the significant safety benefits that the SMS was designed to achieve.

**SMS** = Safety + Financial benefits.

They also report that everyone feels more "engaged" in the business – as well as making the business safer.

Based on the positive safety management system experience gained by flight operations, aircraft maintenance organizations, airports and air traffic management organizations around the world, the International Civil Aviation Organization (ICAO) has introduced the requirement for all commercial air transport operators, non-commercial operators of large and turbojet aircraft, aircraft maintenance organizations, airport operators and air traffic management organizations to develop and implement safety management systems.

It can be expected that national civil aviation rules will soon reflect this requirement.

SMS will be required for:

1. commercial air transport operators,
2. non-commercial operators of large and turbojet aircraft,
3. aircraft maintenance organizations,
4. airport operators, and
5. air traffic management organizations.

# 3. MAKING THE CASE FOR SMS

## 3.1 The Safety Case

### 3.1.1 Basic Safety Concepts

Safety has been defined in this manual as "*the state in which the risk to harm to persons or damage to property is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management*".

The acceptable level of risk within an organization can be expressed by a strategic safety objective. A strategic safety objective expresses the safety expectations of an operator, a service provider or an agency involved in safety oversight. It provides an objective in terms of the safety performance that operators or service providers seek to achieve while conducting their core business functions. It should be a performance based reference against which safety performance can be measured. In developing a strategic safety objective, it is necessary to consider such factors as the level of risk that applies in the operating environment, the cost and benefits of improvements and the expectations of the stakeholders.

**Strategic safety objective** must consider the:

- level of risk that applies in the operating environment,
- cost and benefits of improvements to the system,
- expectations of the stakeholders, and
- expectations of the regulator.

### 3.1.2 Traditional Approach

In the traditional approach to safety, when an accident occurred, questions were asked such as:

- How and why did competent personnel make the errors necessary to precipitate the accident?
- Could something like this happen again?

In the past it often was the practice of investigators to examine the chain of events or circumstances that ultimately led to someone doing something inappropriate, thereby triggering the accident.

This inappropriate behavior may have been an error in judgment (such as the belief that a bad situation was salvageable), an error due to inattention (such as an error that may have been related to a heavy workload or preoccupation with another activity, or a deliberate violation of procedures or rules (such as deviation from standard operating procedures (SOPs)).

The investigative focus was more often than not on finding "the root cause" of the accident and this often led to blaming and sometimes punishing, someone for "making the error" that "caused" the accident. At best, safety management efforts concentrated on eliminating human error.

An example is the issue of runway incursions. In the past, runway incursions may have been attributed to human error. *"The pilot failed to adhere to the clearance and entered the runway without clearance*", or "*the controller made an error when he or she issued the clearance*". So efforts to resolve the problem may have focused on the elimination of errors in the delivery and receipt of clearances.

However, the errors or violations that trigger accidents often seem to occur randomly. With no particular pattern to pursue, such safety management efforts to reduce or eliminate random events are usually ineffective. Besides, humans err - even highly qualified, highly motivated professionals. It is unrealistic to try to *eliminate* human error. Rather, we have learned that we need to predict how error can occur, and manage the circumstances to reduce the probability of those errors, and to manage the results when they do occur. Accordingly, the focus changes from 'human error' to 'human factors'.

Analysis of accident data all too often reveals that the situation prior to the accident was *"*ripe for an accident*"*. Safety-minded persons may even have been saying that it was just a matter of time before these circumstances led to an accident. When the accident occurred, often healthy, qualified, experienced, motivated and well-equipped personnel were found to have committed errors that triggered the accident.

They, and their colleagues, may have committed these errors or unsafe practices many times before without adverse consequences. In addition, some of the latent conditions in which

they were operating may have been present for years, again without causing an accident.

Sometimes these latent conditions are the consequence of decisions made by management. They recognized the risks but other priorities required a trade-off. At other times, the hazards and risks are not recognized by the decision-makers. Indeed, front-line personnel often work in a context that is defined by organizational and management factors beyond their control. The front-line employees are merely part of a larger system – the persons who act out the decisions made in a boardroom.

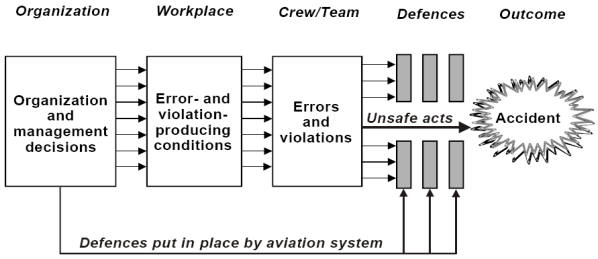
To be successful, safety management systems require an alternative understanding of accident causation — one that depends on examining the total context, that is, "the system", in which people work.

### 3.1.3 What is Changing?

Research during the past twenty years has clearly demonstrated that accidents are related to breaches of the defenses that are established to manage the hazards and associated risks inherent in a specific operation or in the aviation industry as a whole.

The Accident Causation Model developed by Professor James Reason is a graphic depiction of this accident causation understanding. This model recognizes that most accidents are "organizational" in nature.

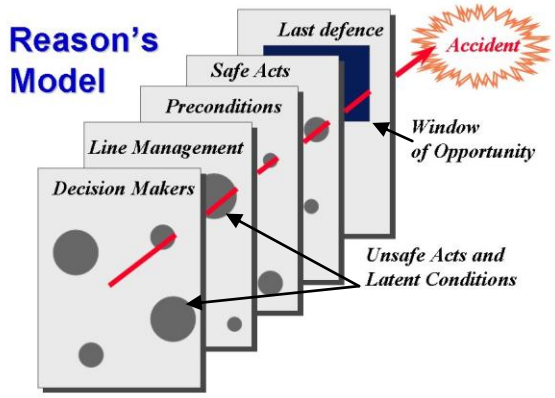
**Accident Causation Model**




**Latent Condition + Active Failures = Accident**

Here is another depiction of his model. In this image he depicts the decision makers within the system as the first line of defense.

The **Decision Makers** in a company with an SMS must be aware that there are *hazards* and associated *safety risks* in the system, so they can develop and implement policies and make decisions to manage, and thereby *mitigate,* the known hazards and associated risks. **Line Managers** then implement the policies and decisions and develop and implement procedures with the same objective.




**Preconditions** (such as minimum professional qualifications and hiring and training standards) are set to ensure that the policies and procedures are appropriate to the operating environment, so the safety risks can be effectively managed. All these standards, policies and procedures may be well designed, but they frequently have gaps or holes in part because they do not integrate or "come together. The **Safe Acts** of the people in the system are a powerful defence. Also there is a **Last Line of Defence** which may include people, equipment or technology.

Sometimes not all of the hazards and associated risk have been identified or correctly understood. These constitute the latent conditions discussed previously that often are the *system safety deficiencies* that permit the hazards to exist again and again.

System safety deficiencies are the circumstance that permits hazards of a like nature to exist.

Various defenses are built into the system to protect against inappropriate performance, poor decisions or other threats to the safety of the system. The model also recognizes that the decisions that created the defenses can also create **latent conditions** that could lead to an accident.

The **latent conditions** exist because of issues such as poor design, gaps in supervision, undetected defects or maintenance failures, unworkable procedures, poor training, conflicting goals and objectives, etc. They then combine with, or cause, **active failures**, such as errors or

violations of procedures that produce an accident.

These **latent conditions** may have their origin in management decisions that were made with good intentions and were based on the best available information, but have unintended consequences. They may include issues such as staffing levels, work schedules, operating procedures, to name just a few.

When we add the people who "do" the work to the systems – pilots, aircraft maintenance personnel and others in the operation – another dimension is added because it is certain that people will make errors and slips, suffer lapses and commit violations in the course of their duties.

***Slip***

- An action that is not carried out as planned
- Will be evident

***Lapse***

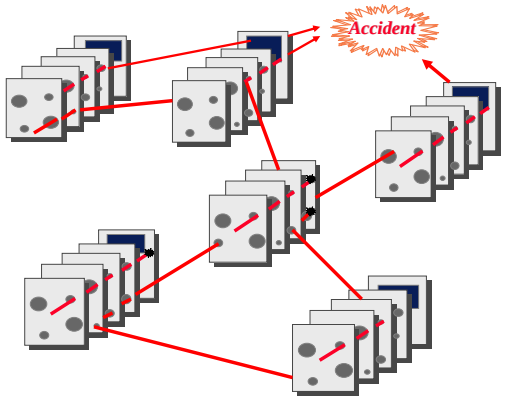
- A failure of memory
- May not necessarily be evident

**Violation -** Deliberate act contrary to a procedure or a "work around".

These are the **unsafe acts**, which are also hazards – the condition or circumstance that can lead to loss. When all of the holes in the **defenses** left by the latent conditions line up with the active failures, the **defenses** are breached, and an accident or incident can occur. In this way, we can see how the four terms we used to understand risk management (i.e. system safety deficiencies, hazards, risk and mitigation) "map out" on James Reason's model of accident causation. We can clearly see that we need a system to manage hazards and risks to reduce the likelihood of an accident from occurring.

More information on human error considerations is contained in Appendix B.

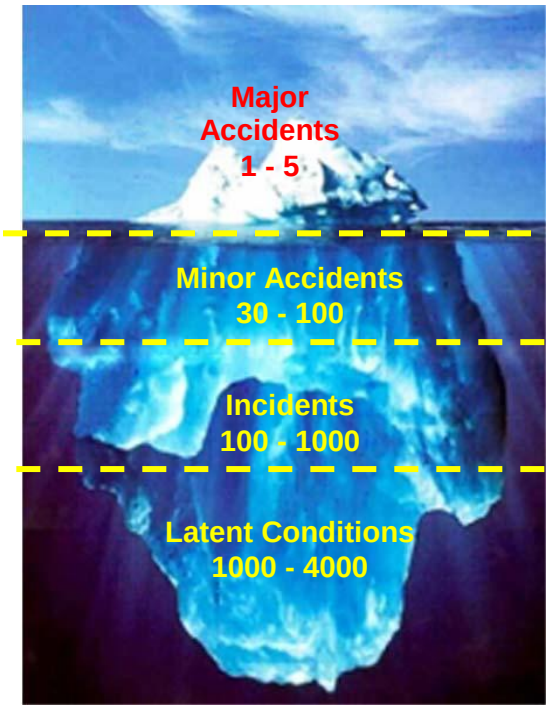
The real world of aviation is seldom as simple as the two-dimensional depictions of this model. Rather, it is a complex interaction between systems, each with their own latent conditions and potential for active failures. A typical aviation operation with sub-systems involving aircraft operations, aircraft, maintenance, dispatch, air traffic control, airports, FBOs, etc. suddenly doesn't appear as 'simple' as we may believe.




**Typical Aviation System**

There are always precursors to accidents. A fatal accident is the tip of the iceberg. Below the tip lie precursors that may include a few accidents involving serious injury, a number of accidents involving property damage, numerous related incidents with no injury or damage and a host of latent conditions.

All too often these precursors are only recognized after an accident. These precursors, or latent conditions, can be identified through an objective, in-depth hazard identification and risk management process.



Accidents and incidents occur within a defined set of circumstances and conditions. These include the aircraft and other equipment, the weather, the airport and flight services, as well as the regulatory, industry and corporate operating climate. They also include the permutations and combinations of human behavior. At any given time, some of these factors may align in such a way as to create conditions that are ripe for an accident.

Understanding the context in which accidents occur is fundamental to safety management. Some of the principal factors shaping the context for accidents and incidents include equipment design, supporting infrastructure, human and cultural factors, corporate safety culture and cost factors.

### 3.1.4 An Evolving Understanding of Safety

The business aviation community has historically experienced a very low accident rate. That safety record has largely been the result of a series of technological advances and operational and regulatory activities.

To sustain safety at this exemplary level as aviation activity increases, safety management practices are shifting from a reactive mode to a more **proactive** mode. In doing this a number of factors have been found to be effective. They include:

- application of scientifically-based risk management methods,
- senior management's commitment to the management of safety,
- a corporate safety culture that fosters safe practices, encourages safety communications and actively manages safety with the same attention to results as financial management,
- effective implementation of standard operating procedures (SOPs), including the use of checklists and briefings,
- a non-punitive environment (or just culture) to foster effective incident and hazard reporting,
- systems to collect, analyze and share safety-related data arising from normal operations,
- competent investigation of accidents and serious incidents identifying systemic safety deficiencies (rather than just targets for blame),
- integration of safety training (including human factors) for operational personnel,
- sharing safety lessons learned and best practices through the active exchange of safety information among companies and regulatory authorities, and
- systematic safety oversight and performance monitoring aimed at assessing safety performance and reducing or eliminating emerging problem areas.

No single element meets today's expectations for risk management. Rather, an integrated application of these elements will reduce the occurrence of unsafe acts and improve the management of latent conditions within an operation.

If we go back to our runway incursion example and apply these proactive principles, we come up with a significantly different solution than simply blaming it on pilot or controller error. Today we are using a number of these proactive safety management principles to address the issue. They include:

- analyzing the airport, air traffic control and cockpit environments to identify the risk related to the runway incursion hazard,
- identifying latent unsafe conditions within those environments related to the hazard,
- engaging senior management of airports, air traffic management, regulatory agencies and ICAO in addressing the hazard,
- developing strategies to address risks and latent unsafe conditions,
- ensuring that everyone understands the hazard, associated risks and latent unsafe conditions that exist,
- promoting proven operating practices,
- deploying specialized equipment,
- encouraging reporting of near misses,
- monitoring the results of these efforts, and
- investigating runway incursion incidents and accidents.

However, it must be understood that while effective safety management will significantly reduce the risk of an accident, there can never be a guarantee that all accidents will be prevented. This would require a risk- and hazard-free environment that is impossible when

humans use highly complex technological systems to provide aviation services.

## 3.2 Operational Case

If we carefully consider what we have discussed about accident causation in the context of modern aviation and the complexity of interdependent systems and operator interface issue in the operational environment, it is evident that operations will benefit significantly from a comprehensive, proactive approach to safety management. We can systematically anticipate, and therefore manage, the breaches in the defenses that increase the likelihood of an incident or accident.

**Operational Case**

- Technological complexity
- Operator – equipment interface complexity
- Interdependency of complex technological systems

## 3.3 Business Case

Increased global competitiveness and the pressures on businesses to control costs at all levels requires operators to maximize efficiency while conducting safe operations. To do that we must ensure that we have identified all of the hazards and associated risks inherent in the operation and then introduced mitigation to reduce them to a level as low as reasonably practicable.

If we do not have good data upon which to base safety management decisions and systems to track the appropriateness and effectiveness of our decisions, we may inadvertently ignore the safety risks, or implement defenses that are either unnecessarily strong, or that can be easily breached. If the safety risk is ignored, the first indication of inadequate defenses may be an accident. The implementation of overly aggressive defenses can result in the significant waste of scarce resources. A well-managed safety management system is a powerful tool for the maximization of resource efficiency and effectiveness.

The cost of insurance and the potential liability in the case of an accident is also a strong motivator to effectively manage safety. Also, in the unfortunate case of an accident, the need for an operator to demonstrate due diligence cannot be overstressed.

**Business Case**

- Increased global competitiveness
- Requirement for efficient and safe operations
- Requirement to maximize resource efficiency and effectiveness
- Liability and cost of insurance
- Need for business to demonstrate “due diligence”

# 4. INTRODUCTION TO SAFETY-RISK MANAGEMENT

## 4.1 Understanding Hazard and Risk

### 4.1.1 Key Terms

In their efforts to manage the safety of an operation and reduce the risk of an accident, operators must effectively manage the risks associated with any hazard that cannot be eliminated. It is important to have a clear understanding of several terms and how they are used in safety management and in this document.

**Hazard -** The condition or circumstance that can lead to physical injury or damage.

**Risk** - The consequence of a hazard measured in terms of likelihood and severity.

**Mitigation** -The measures taken to eliminate a hazard, or to reduce the likelihood or severity of a risk.

**System Safety Deficiency** - The circumstance that permits hazards of a like nature to exist.

An obstacle on the end of a runway is a hazard. There are several associated risks. First, an aircraft may hit the obstacle during take-off or landing.

Another risk is that the pilot may know the obstacle is there and, to avoid it, the pilot may carry out a steeper than normal approach and arrive at the end of the runway “hot and high”, continue with the landing and run off the end of the runway.

A third risk could be that the pilot in the last scenario recognizes that he or she is “hot and high” and executes a “go around”.

**Hazard** - An obstacle at the end of a runway

**Risk 1** – Collision with the object

**Risk 2** – Runway excursion related to avoidance action

**Risk 3** – Go around

By drawing on accident and incident data and other available information (such as operational experience), an assessment of the likelihood and severity of each of the three risks associated with the hazard of the obstacle on the end of a runway, can be made. The consequence of striking the obstacle while in flight is likely to be more severe than the aircraft running-off the end of the runway, and both risks will normally cause more damage than a go around.

### 4.1.2 Classification of Severity and Likelihood

From the foregoing it is evident that there are a broad range of potential risks associated with the hazard – the obstacle and the end of the runway. Each of the risks has a different potential severity and a likelihood of occurring. In order to appropriately focus available resources on dealing with the hazard and the associated risks it is necessary to classify them. There are many risk classification systems available ranging from something as simple as the one shown here to more complex systems such as those contained in Appendix C. In any event, it is important to use available data and information to classify the risks.

| **Severity** | |
|---|---|
| Category A | Potential for loss of life or destruction of the aircraft |
| Category B | Potential for serious injury or major damage to the aircraft |
| Category C | Potential for minor injury or minor damage to the aircraft |
| Category D | Trivial (e.g. inconvenience) |

| **Likelihood** | |
|---|---|
| High | Often |
| Medium | Occasionally |
| Low | Seldom |
| Rare | Unlikely |
| Very rare | Highly Unlikely |

Remember that a hazard is the condition or circumstance that can lead to physical damage or loss.

When identifying the hazard do not confuse it with the associated risks. As we discussed earlier, the obstacle on the end of the runway was the hazard. There were three risks associated with that hazard. The first risk to safety was that an aircraft might hit the obstacle while taking off or landing. The second risk was that the pilot may know the obstacle was there

and in order to ensure the aircraft does not hit the obstacle, he or she may carry out a steeper than normal approach and arrive at the end of the runway "hot and high", continue with the landing and run off the end of the runway. A third risk that was identified was that the pilot in the second scenario may recognize that he or she is hot and high and execute a "go around".

In the same vein, fatigue is a hazard that is an underlying condition for many forms of human error (unsafe acts) that, in turn, can lead to a number of risks.

It is important to dig deep into the scenario to ensure that the underlying hazards are identified.

***Identify the hazards and risks embedded in the event scenarios***

Once the hazards and associated risk are understood, potential courses of action to manage them should be explored. One course of action may be to eliminate the hazard (the obstacle at the end of the runway) by removing it. If that cannot be done, a second course of action may be to avoid the hazard by not using the runway. The hazard remains, but the likelihood of it being struck by aircraft during take-off or landing is reduced.

A third course of action is to develop and implement mitigation to reduce the three identified risks to an acceptable level.

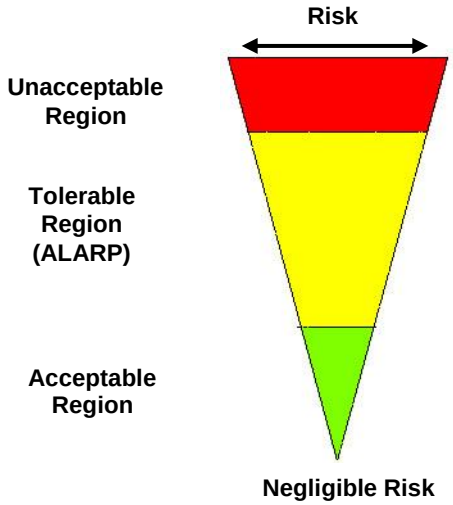
**Risk Management Options**

1. Remove obstacle,
2. Not use the runway, or
3. Develop mitigation to reduce the risks to an acceptable level.

The third course of action requires the operator to predetermine criteria regarding the acceptable level of risk and to assess the benefits of the operation versus the risks involved.

In assessing risk and developing mitigation, the risks are often considered in three broad categories.

1. The risks are so high that they are **unacceptable**.
2. The risks are so low that they are clearly **acceptable**.
3. The risks are between the two categories and consideration needs to be given to managing the risks so the benefits can be realized.




If the risk does not meet the predetermined acceptability criteria, an attempt must always be made to reduce it to a level that is acceptable by using appropriate mitigation procedures.

If the risk cannot be reduced to or below the fully acceptable level, it may be regarded as tolerable if:

- the risk is less than the predetermined unacceptable limit;
- the risk has been reduced to a level that is as low as reasonably practicable; and
- the benefits of the activity or operation are sufficient to justify accepting the risk.

## 4.2 ALARP

The acronym **ALARP** is used to describe a risk that has been reduced to a level that is ***as low as reasonably practicable***. In determining what is "reasonably practicable" consideration should be given to both the technical feasibility of further reducing the risk, and the cost. This might include some level of cost-benefit study.

Determining that the risk is as low as reasonably practicable means that any further risk reduction is either impracticable, or is grossly outweighed by the costs. It should, however, be borne in mind that when an individual, operator or society "accepts" a risk, this does not mean that the risk is eliminated. Some level of risk remains. However, the individual, operator or society has accepted that the residual risk is sufficiently low

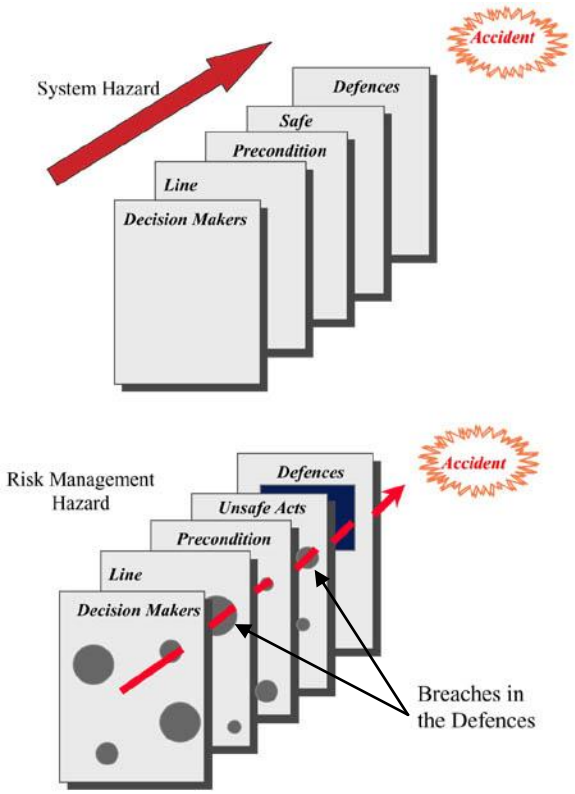
that it is outweighed by the benefits. Regrettably, it often is only after an accident that individuals, operators or a society re-examine the "acceptability" of risk, using hindsight for retrospective analysis.

## 4.3 Risk Management as Part of SMS

A performance-based SMS uses risk management to reduce safety risks to a level as low as reasonably practicable. It does so in a manner that takes full account of Reason's model of accident causation, where latent conditions and system safety deficiencies (i.e. organizational factors) cause hazards to occur and, therefore, lead to risk that needs to be managed. It also is the means by which an SMS is customized to suit the size and complexity of the organization or operation. The following example illustrates.

Human fatigue meets the definition of a hazard – a condition or circumstance that can lead to physical injury or damage. The flight crew of a company that principally operates trans-continental or inter-continental flights on a 24/7 basis would be exposed to the hazard of fatigue - considerably more often than a company that operates on local routes during the more traditional, "normal" working hours. The system hazard can be represented by the arrow in the following figure and, for the 24/7 company, the system hazard arrow could be envisaged as much larger than the system hazard arrow of the "normal working hours" company.

The mitigation strategies to reduce the risk of fatigue in each company would need to differ considerably to reduce the risk of fatigue in each company to a level as low as reasonably practicable. Therefore the defenses (in the form of company policies and procedures for crew scheduling, dispatch methods, minimum rest periods, maximum duty days, aircraft equipment, etc.) as illustrated by the solid, overlapping barriers in the first figure to the right, would be considerably more comprehensive and stringent in the 24/7 company.




Furthermore, information received through SMS processes such as hazard or incident reports, committee meetings, or audit findings that suggest weaknesses in the policies and procedures for managing fatigue may need to be treated with much higher priority than in the "Monday-to-Friday" operation. These breaches in the defense are illustrated by the holes in the fatigue management defenses in the second figure above. A "hole" might be a "one-time" scheduling problem that resulted in a crew member not receiving the minimum rest period. Or it might be more systemic, where on particular routes the crews periodically operate at the limits or beyond the maximum crew duty period. This would be a system safety deficiency that causes the hazard of fatigue to occur regularly.

# 5. THE SMS MANAGEMENT FRAMEWORK

## 5.1 SMS Overview and Definition

As noted earlier, the IS-BAO definition of a safety management system is "*the systematic and comprehensive process for the proactive management of safety-risks that integrates the management of operations and technical systems with financial and human resource management*".

That definition stresses the **"systematic"** nature of an SMS.

The definition also stresses that an SMS is a **comprehensive process**. That is that it is not just a "pilot thing" or a "maintenance thing", but it includes all aspects of the operation, including the commercial and human resource "things".

The purpose of an SMS is identified as the **proactive management of safety-risks.** That reinforces the recognition that an SMS must be always looking forward, not focused on history. Safety must be designed into an organization, and into its operation. Surprises in aviation safety are seldom positive, and an SMS helps to minimize surprises!

The definition also notes that the SMS must not be considered as a stand-alone system for any part of the operation, but that it must integrate all of the systems used to **manage operations, maintenance, finance and human recourses**.

## 5.2 Safety Policy

Senior management support is all-important if a safety management system is to succeed. That is best achieved through the policy development process.

The safety policy is a high-level statement of desired corporate safety performance. The aim is twofold:

1. to provide guidance to everyone in the operation who has a direct or indirect impact on safety performance; and
2. to provide specific direction to ensure that safety management activity is purposeful and directed.

A safety policy generally describes the high-level accountabilities and responsibilities of the owner, CEO or equivalent of a company and the personnel involved in the operation and the measurable standards. It is constructed so that short and long-term safety goals and objectives or "safety performance goals", of the flight department can be linked to the strategic safety objective identified in the safety policy.

Examples of safety policies can be found in the ***Safety Policy Examples*** and the ***ICAO Safety Policy Example*** in the ***IBAC SMS Toolkit***.

While it is recommended that the policy statement be formulated in the early stages of SMS development it may be advantageous to finalize it only at the end of the development process when all aspects of the SMS are completed.

## 5.3 Goals and Safety Management Processes

The strategic objective of an SMS should be performance based, that is it describes what is to be achieved rather than how, and as such it usually is ongoing. For example a logical strategic safety objective would be to reduce risk to a level as low as reasonably practicable. This recognizes that there is significant risk inherent in aviation and, while it makes good business sense to reduce risk and avoid the very high costs associated with an accident, it would be prohibitively expensive and detrimental to the business environment if an operator were to try to eliminate all risks. Therefore, the operator must attempt to optimize safety performance in an operational and business environment through:

- proactive identification of hazards,
- assessment and measurement of associated safety-risks,
- taking action to mitigate the hazards and risks by either eliminating the hazards or reducing the associated risks to an acceptable level,
- tracking the mitigation activities to verify that they are appropriate and effective, and
- if required, modifying the mitigation activities.

A good example to illustrate this is the hazard of fatigue in flight operations. We know from research that any time that people work long hours or outside of their natural circadian rhythm the hazard of fatigue is present. If we limited flight crews to working eight hours a day

between 8 a.m. and 6 p.m. we could virtually eliminate the safety risks associated with the hazard, but in most situations we certainly would not have a very effective operation.

Instead it is more appropriate to use the steps described above to ensure that the factors that contribute to fatigue are well known and that we develop a fatigue countermeasure program to reduce the risks to an acceptable level.

It is necessary that an SMS have long-term and ongoing safety objectives and short term goals that are continuously reviewed and regularly updated. This is an important part of ensuring that the safety management activities remain focused and relevant. These objectives and goals should be measurable and realistic. The establishment of good goals lies in appreciating what is manageable and what is not. It is important to recognize that in aviation while it is possible to minimize safety risks it is not possible to eliminate them. Therefore, rather than use ”zero accidents” as the goal, the goals should emphasize what needs to be done to explicitly demonstrate that safety risks are being managed to a level as low as reasonably practicable.

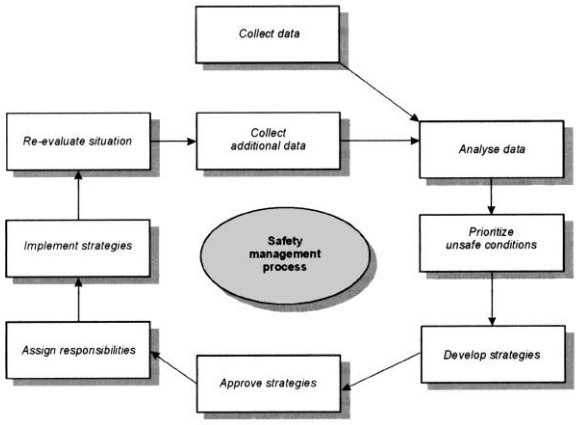
Accordingly, it would be appropriate to have long term objectives that relate to overall enhancement of safety and maturation of the safety management system and annual goals that reflect what is being done to get there. For example, the establishment of a strong corporate safety culture is a realistic long term objective. To move toward that objective, the goals for the year may include something such as the following.

- Ensure that all personnel understand the hazards and risks inherent in their area of operation, by briefing everyone on the safety-risk profile and by holding monthly meetings to discuss all hazard reports and their disposition.
- Foster an open and reporting culture by ensuring that all hazard identification and tracking reports are received in a positive manner and that feedback is provided as soon as possible - at least within two weeks.
- Foster a just culture by ensuring that all personnel know and agree upon what is acceptable behavior and what is not through publication of a just culture policy statement. The policy statement will be developed in a consultative manner that involves all personnel.

These objectives and goals should relate to the strategic safety objective identified in the safety policy.

## 5.4 Safety Management Process

The following diagram can be used to further describe the safety management process.




The safety management process is data driven. The data that are collected help determine safety performance, and can be used to identify hazards or system safety deficiencies. The data may be found anywhere: the operating environment, the equipment used, the people involved in the operation, work procedures, the human/equipment/procedures interactions, etc.

By analyzing all the pertinent information, safety hazards can be identified. The conditions under which the hazards pose real risks, their potential consequences and the likelihood of occurrence can be determined; in other words, *What* can happen? *How?* and *When?* This analysis can be both qualitative and quantitative.

A risk analysis process determines the seriousness of hazards. This determination may require a cost/benefit analysis.

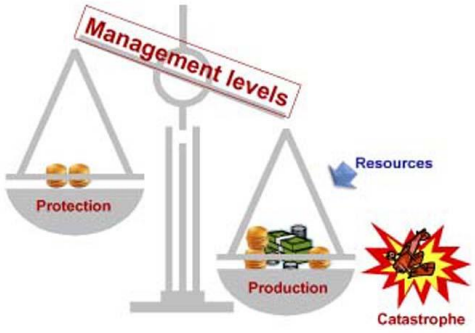
Beginning with the highest priority risks, several options for managing the risks may be considered, for example:

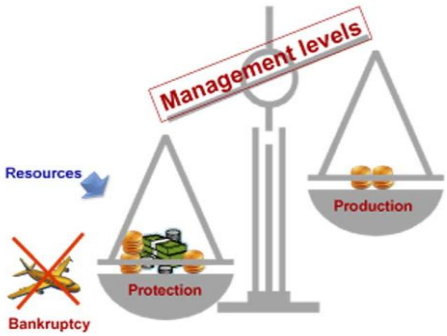
- **Spread** the risk across as large a base of risk-takers as practical. This is the basis of insurance.
- **Eliminate** the risk entirely (possibly by ceasing that operation or practice).
- **Accept** the risk and continue operations unchanged.
- **Mitigate** the risk by implementing measures to reduce the risk or at least facilitate coping with the risk.

In "real life", a company's strategy often includes combinations of these options: exposure to a hazard will be minimized (but not eliminated); mitigation measures will be introduced; other stakeholders will be involved in managing the risks (e.g. ATC may provide operational information to crews, or aircraft manufacturers may modify equipment to suit the industry's needs, and the resulting operation will be insured).

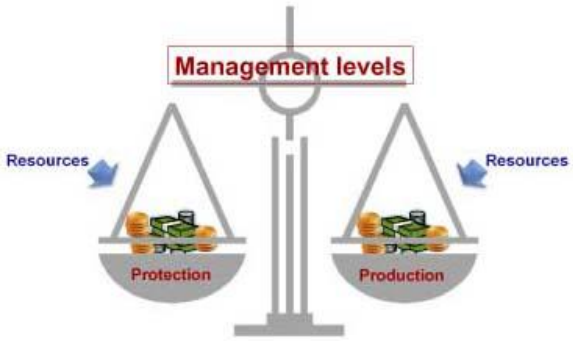
When developing a risk-management strategy, care is required to avoid introducing new hazards that, unidentified and unmanaged, could result in an unacceptable level of risk.

Having analyzed the risks and decided on an appropriate course of action, management's approval is required to proceed. Traditionally, the challenge in this step has been formulating a convincing rationale for what may be expensive change. The use of safety-risk management data to make decisions in companies with an SMS can reduce the traditional competition between "production objectives" and "protection objectives". With a well-developed SMS it is much easier to strike an appropriate balance and ensure a good return on safety investment.




Balance can be achieved with a sound SMS




Following the decision to precede with SMS development the "nuts and bolts" of the process must be worked out. This includes a determination of resource allocation, assignment of responsibilities, scheduling, revisions to operating procedures, etc.

Implementation may not be as successful – or as easy - as initially envisaged. So there must be mechanisms to get feedback to close the information loop.

- What new problems may have been introduced?
- How well is the agreed strategy for risk reduction meeting performance expectations?
- What modifications to the system or process may be required?

Depending on the re-evaluation step, new information may be required and the full cycle may need to be reiterated to refine the safety action.

Safety management requires analytical skills that may not be routinely practiced by management. The complexity of the problem will determine the most appropriate analytical tool. The closed-loop process of safety management

also requires feedback to ensure that management can test the validity of its decisions and assess the effectiveness of their implementation. This often comes from simple tools like hazard reports, committee meetings, incidents reports, regulatory observations, etc.

The net result should be an SMS that is:

- proactive,
- purposeful and comprehensive,
- appropriate to the size and complexity of the operation,
- effective, and
- explainable to all persons involved.

## 5.5 Management's Role in SMS

As was previously noted, an SMS is first and foremost a management system. As such, the management of the flight operation must be fully engaged in the process and demonstrate leadership and their commitment. They must have the complete support of the highest level in the company and this support must be articulated through a clear policy statement that:

1. includes a commitment to safety as a core value,
2. identifies a strategic safety objective, and
3. sets a direction through credible policies, objectives, goals & standards.

Management must also commit to provide adequate resources, including sufficient time to fulfill assigned tasks safely and efficiently, and ensure that the expertise, including knowledgeable individuals, resource material and training, is available.

By doing so, management will foster a safety culture throughout the organization. This is more fully discussed in section 10.1.

To assist senior management understating their role in an SMS see the CASA publication Safety Management for CEOs and the Transport Canada publication Selection of the Accountable Executive.

## 5.6 Roles, Responsibilities and Accountabilities

There should also be clear identification of the people who are responsible for related activities and their accountabilities within the safety management system. These accountabilities should also be reflected in the safety policy.

Accountabilities can be thought of as the sum of duties and responsibilities. The following are examples of accountability statements for a non-commercial corporate operation.

- The CEO, owner or accountable executive, is accountable for providing the resources required to conduct a safe operation and to implement and maintain the SMS.
- The flight department manger, or director of operations, is accountable for the safety of the operation.
- The chief pilot is accountable for the aircraft operating standards and procedures and implementing the related aspects of the SMS.
- The chief of maintenance is accountable for the airworthiness of the aircraft and implementing the related aspects of the SMS.
- The staff members are accountable for carrying out their duties in accordance with approved procedures and for participating in the safety management system.
- Passengers are accountable for complying with regulations, company policies and crew member instructions, as well as participating in operator hazard reporting programs and safety related training programs.

It is important that everyone involved in the operation clearly understand their duties, responsibilities and accountabilities. Ensuring that this is the case should be part of the safety management strategy.

# 6. HAZARD ANALYSIS AND RISK MANAGEMENT

## 6.1 General Considerations

One proven way to conduct a hazard analysis is to engage as many of the people involved in the operations as is practical and use the following process.

1. Brainstorm event scenarios. That is, identify the event or series of events that could lead to an accident and then assign priorities to categorize the most likely and serious.
2. Identify the hazards embedded in the event scenarios.
3. Classify similar events and similar hazards.
4. Determine the associated risks and assess their severity and likelihood.
5. Identify and system safety deficiencies,
6. Document the hazard identification.

Once the hazards are identified and analyzed the next step is to develop mitigation. The mitigation process is discussed in section 6.4.
In this process it is important to recall the definitions of hazard, risk and mitigation.

A **hazard** is the condition or circumstance that can lead to physical injury or damage.

A **risk** is the consequence of a hazard measured in terms of likelihood and severity.

**Mitigation** is the measures taken to eliminate a hazard, or to reduce the likelihood or severity of a risk.

A **system safety deficiency** is the circumstance that permits hazards of a like nature to exist. It is almost always similar to a "latent condition".

An example of a system safety deficiency could be the result of a decision that was made in response to financial pressures and personnel shortages to reduce air traffic controller staffing levels without a comprehensive risk assessment. Such a situation could result in a broad number of like hazards within that air traffic control system.

## 6.2 Conducting a Hazard Analysis

### 6.2.1 Hazard Identification and Analysis

A few basic steps are required before starting the hazard identification and analysis.

First identify precisely what it is you are going to analyze.

If the hazard analysis is being conducted to create or update the safety-risk profile for the operation, then ensure that all aspects of the operation are included in the process. That will require people from all segments of the operation to be involved.
It is recommended that the scope of the process be written down and kept handy so that it can be referred to when conducting and documenting the analysis

Next determine who will do the analysis. One or more persons who know each of the aspects of the operations should be included. The person or persons, must be experienced and credible, and preferably have first-hand and current knowledge of the operational conditions. The person, or persons, should also be good at "thinking outside of the box". Where a flight department is very small it may be advantageous to involve people with appropriate expertise from outside the operation.

Provide all information that is available to the people who will be involved in the process. The information should include guidance on the process, the scope of the analysis and any safety related data that is available. The document *Guidelines for the Conduct of Risk Analysis* that is included on the IS-BAO CD can be useful guidance for the process.

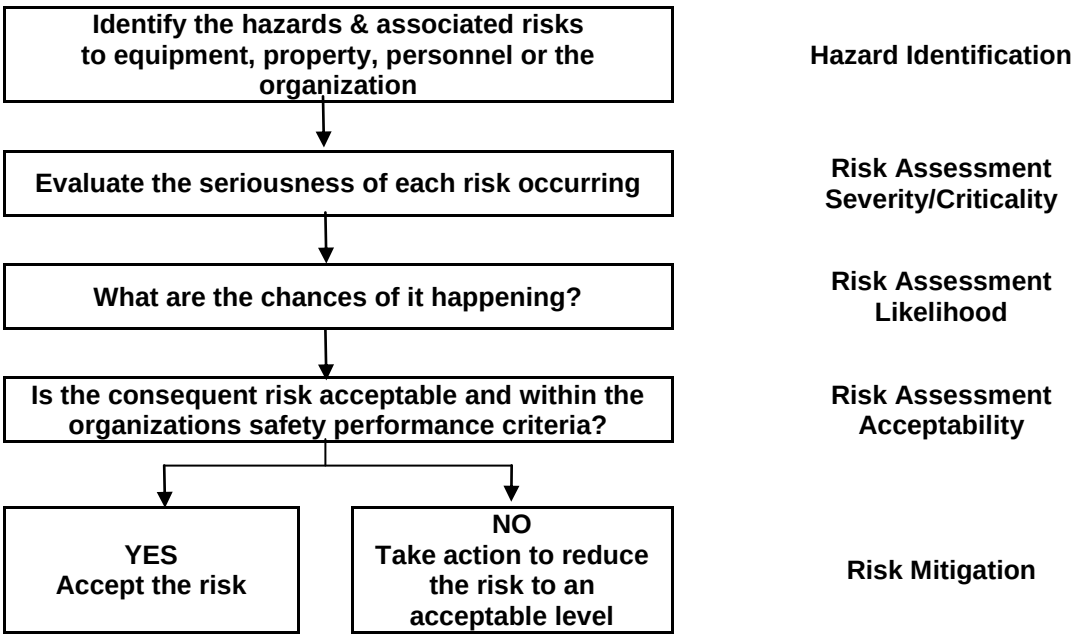
Make sure you are ready and have suitable facilities. They should include an appropriately-sized room and a means of recording information as you move through the analysis. A good recording method is an old-fashioned flip chart with markers and masking tape. Of course the information can also be recorded electronically. Also, make sure that the group will not be uninterrupted so they can stay focused while doing and documenting the analysis.

The checklist that is included in the IS-BAO *Guidelines for the Conduct of Risk Analysis* and in the ***Hazard Identification Tools*** in the ***IBAC SMS Toolkit*** can be used when planning and conducting a hazard identification and analysis.

| Planning the Hazard Analysis | Completed | Notes |
|---|---|---|
| 1. Determine scope | | |
| 2. Pick team | | |
| 3. Plan logistics | | |
| • date(s) and times | | |
| • room | | |
| • flip charts, etc | | |
| • forms | | |
| 4. Inform team | | |
| 5. Other | | |

During the hazard identification you will identify key hazards and the associated risks, and develop mitigation so that the chances of having a serious accident are minimized. The following is a flow diagram that depicts the process.

**Hazard Identification and Risk Analysis Process**




The following checklist, which is also included in the ***Hazard Identification Tools*** in the ***IBAC SMS Toolkit,*** may be of use in organizing the hazard identification.

| Conducting the Hazard Analysis | Completed | Notes |
|---|---|---|
| 1. Brief the team | | |
| 2. Brainstorm accident scenarios | | |
| 3. Categorize scenarios by priority | | |
| 4. Identify the hazards | | |
| 5. Cluster similar events & hazards | | |
| 6. Develop mitigation | | |
| 7. Determine likelihood & severity | | |
| 8. Review mitigation to verify that it is appropriate | | |
| 9. Document | | |
| - event form | | |
| - hazard forms | | |
| - safety-risk profile | | |

Before starting, review the steps and ensure that everyone is comfortable with what they will be doing and that they realize the important role they will play. Write out the definitions of ”hazard”, ”risk” and ”mitigation” where everyone can refer to them and describe the scope of the process.

***Brainstorm accident scenarios***

Encourage team members to think of and describe accidents that could happen in their operation. Don’t dwell on the details. Just get enough information that the other team members understand the circumstances leading to the event. Jot down the information on a flip chart (one event per flip chart) and move on to the next event.

Hang the flip chart where it can be referred to when needed.

At this point all that needs to be done is to identify the hazards that were involved in the accident scenario. The associated risks will be assessed later.

There are a number of ways of making sure that the list of events is complete. After the team has completed the initial surge of possible scenarios, get them to concentrate on different aspects of the operation. For instance, depending on the nature of the analysis, focus their thinking on previous incidents, seasonal operations, specific aerodromes, different types of operations such as uncontrolled airspace, VFR operations, RVSM, MNPS, different aircraft types, if applicable, etc.

It may be also helpful revisit the accident causation model that was discussed in section 3.1.3 and the principal factors that shape the context for accidents. Information on human factors consideration contained in Appendix B and in the SHEL model in section 6.3 may also be of assistance.

This exercise will normally result in a few more scenarios being identified. Assure everyone that they can always come back and identify other events later.

### 6.2.2 Classification of Severity and Likelihood

The next step is to guide the team in generally classifying the accident scenarios in the order they are more likely to occur and those with the most serious results. A table such as this may be used. Do not spend a lot of time on this, as you will return later to categorize events and hazards more precisely.

| **Severity** | |
|---|---|
| Category A | Potential for loss of life or destruction of the aircraft |
| Category B | Potential for serious injury or major damage to the aircraft |
| Category C | Potential for minor injury or minor damage to the aircraft |
| Category D | Trivial (e.g. inconvenience) |
| | |
| **Likelihood** | |
| High | Often |
| Medium | Occasionally |
| Low | Seldom |
| Rare | Unlikely |
| Very rare | Highly Unlikely |

Now return to the first event scenarios, and discuss in more detail the conditions or circumstances that might align to cause the possible accident. These are potential hazards. Write each hazard down on the flip chart related to the event being discussed. Make sure there is consensus on the hazards, and how they interact to lead to each potential accident.

Remember that a hazard is the condition or circumstance that can lead to physical damage or loss.

When identifying the hazard do not confuse it with the associated risks. In the example provided earlier, the obstacle on the end of the runway was the hazard. There were three risks associated with that hazard. The first risk to safety was that an aircraft might hit the obstacle while taking off or landing. The second risk was that the pilot may know the obstacle was there and in order to ensure the aircraft does not hit the obstacle, he or she may carry out a steeper than normal approach and arrive at the end of the runway "hot and high" - continue with the landing and run off the end of the runway. A third risk that was identified was that the pilot is the second scenario may recognize that he or she is hot and high and executes a "go around".

In the same vein, fatigue is a hazard that is an antecedent condition for many forms of human error (unsafe acts and omissions) that, in turn, can lead to a number of risks.

It is important to dig deep into the scenario to ensure that the underlying hazards are identified.

Continue identifying all the hazards embedded in each event scenario, and write them down on the flip chart. The form in the ***Hazard Identification Tools*** in the ***IBAC SMS Toolkit*** may also be used.

Then identify the risks associated with each hazard that contributed to the accident scenario. Write them on the flip chart too.

| **Accident Scenario Form** | |
|---|---|
| **Event Number** | |
| **Accident Scenario** | |
| **Hazard #1** | |
| **Risk #1** | |
| **Risk #2** | |
| **Risk # 3** | |
| **Hazard #2** | |
| **Risk #1** | |
| **Risk #2** | |

***Categorize similar events and hazards***

The next step is to categorize similar events and hazards in order to identify the circumstances in your operation that cause the most severe and likely risks, and determine if there are key hazards that show up again and again. This information is useful for preparing the safety-risk profile, and leads directly to the development of mitigation that is appropriate to the risks in your operation.

When examining similar hazards, categorize them in terms of whether they are operational, technical, environment, or related to human factors.

***Categorize similar events and hazards***

Operational – Mid-air collision

Technical – Unintentional dispatch of an unserviceable aircraft

Environment – The obstacle at the end of the runway

Human Factors – A slip or lapse

Also determine whether there is an underlying circumstance that might be causing the hazards. This is called a system-safety deficiency. It is a circumstance that permits hazards of a like nature to exist, and usually is based in decisions that have been made about the way the operation is conducted. Examples of potential system safety deficiencies might include:

- regularly operating an aircraft type into a location with a single runway that barely meets the aircraft's certification requirements;
- hiring and crewing pilots with limited experience in the operating conditions; and
- providing knowledge-based training when skill-based training is essential.

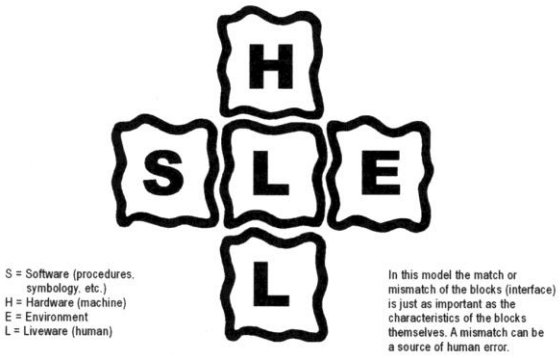
It is also appropriate to consider the degree of exposure to the hazard. The nature of some operations may have a higher level of exposure to the hazard of fatigue and frequency of operations into certain airport may result in increased exposure to certain hazards.

## 6.3 The SHEL Model

### 6.3.1 Understanding SHEL

The workplace typically involves a complex set of interrelated factors and conditions, which may affect human performance. The SHEL model can be used to depict the interrelationships among the various components of the aviation system. It is an easy way to identify hazards, for instance during a hazard analysis described in section 6.1. This model is a development of the traditional "man-machine-environment" system. It focuses on the human being and the human's interfaces with the other components of the aviation system (e.g. the equipment the person uses, or the working conditions experienced when using that equipment). The SHEL model's name is derived from the initial letters of its four components:

- ***Liveware*** for humans in the workplace;
- ***Hardware*** for machine and equipment;
- ***Software*** for procedures, training, support, etc.; and
- ***Environment*** for the operating circumstances in which the rest of the Liveware, Hardware and Software system must function.




This building block diagram is intended to provide a basic understanding of the relationship of the human to other factors in the workplace. It can be useful when *proactively* identifying hazards in a future operation (i.e. when conducting a hazard analysis), or for understanding why things have gone wrong (e.g. when receiving a hazard report) in the existing operation.

In the centre of the SHEL model are those persons at the front line of operations. Although people are remarkably adaptable, they are subject to considerable variations in performance. Humans have strengths. Humans have limitations. We must manage both, optimizing the former while "coping" with the latter.

The behavior of humans can never be completely standardized, therefore, it must be recognized that the edges of this block and the blocks humans interface with are not simple and straight. To reduce the opportunity for humans to compromise technical or operational performance, the effects of irregularities at the interfaces with the various "SHEL" blocks must be anticipated and understood. The other components of the system must be carefully matched to humans, or hazards will exist.

**Liveware Factors**

There are several different aspects of the human factor – the Liveware. Some of the more important factors affecting individual performance are:

***Physical factors:*** These include the individual's physical capabilities to perform the required tasks, such as strength, height, reach, vision and hearing.

***Physiological factors:*** These include those factors that affect the human's internal physical processes that can compromise a person's physical and cognitive performance, such as oxygen availability, general health and fitness, disease or illness, tobacco, drug or alcohol use, personal stress, fatigue and pregnancy.

***Psychological factors:*** These include those factors affecting the psychological preparedness of the individual to meet all the circumstances that might occur, such as adequacy of training, knowledge and experience, and workload. The individual's psychological fitness can include such factors as motivation, judgment, attitude towards risky behavior, confidence and stress.

***Psycho-social factors:*** These include all those external factors in the social system that can cause pressure on individuals in their work and non-work environments, such as an argument with a supervisor, labor-management disputes, a death in the family, personal financial problems or other similar sources of domestic tension.

The shell model can be helpful in visualizing the interfaces between the various components of the aviation system. These interfaces include:

The ***Liveware-Hardware*** interface between the human and the machine (ergonomics) is the one most commonly considered when speaking of human factors. It determines how the human interfaces with the physical work environment, such as the design of seats to fit the sitting characteristics of the human body, displays to match the sensory and information processing characteristics of the user, and proper movement, coding and location of controls for the user.

However, as we said earlier, humans have strengths, and one of these is their resiliency. There is a natural human tendency to respond adapt to Liveware - Hardware mismatches. This can be a strength, but it also may mask serious deficiencies, which, too often, only become evident after an accident. A hazard analysis allows us to anticipate and manage these mismatches that have become system safety deficiencies.

The ***Liveware - Software*** interface is the relationship between the individual and the supporting systems found in the workplace, such as the regulations, manuals, checklists, publications, SOPs and computer software. It includes such "user friendliness" issues as currency, accuracy, format and presentation, vocabulary, clarity and symbology.

The ***Liveware-Liveware*** interface is the relationship between the individual and other persons in the workplace. Flight operations personnel, aircraft maintenance personnel and other people function as groups, and group influences play a role in determining human behavior and performance. This interface is concerned with leadership, cooperation, teamwork and personality interactions. The advent of crew resource management (CRM) has resulted in considerable focus on this interface.

CRM training and its extension to other team members within the operation promotes teamwork and focus on the management of normal human errors.

Staff/management relationships are also within the scope of this interface, as are corporate culture, corporate climate and company operating pressures, which can all significantly affect human performance.

The **Liveware-Environment** interface involves the relationship between the individual and the internal and external environments. The internal workplace environment includes such physical factors as temperature, ambient light, noise, vibration and air quality. The external environment for pilots includes such factors as visibility, turbulence and terrain. Modern long-range aircraft and, in some instances, a 24/7 aviation work environment – particularly in aircraft maintenance - includes disturbances to normal biological rhythms and sleep patterns. In addition, the aviation system operates within a context of broad political and economic constraints that in turn affect the overall corporate environment. Included here are such factors as the adequacy of physical facilities and

supporting infrastructure, the local financial situation, and the regulatory environment. Just as the immediate work environment may create pressures to take short cuts, inadequate infrastructure support may also compromise the quality of decision making.

Care needs to be taken in order that hazards do not "fall through the cracks" at the interfaces. This will be an important goal of your safety management system.

#### 6.3.2 Using SHEL in a Hazard Analysis and the SMS

The SHEL model is a very good means to systematically identify hazards. It can be used during a hazard analysis, as described in section 6.1. It can also be employed to understand some of the circumstances that may be "causing" a hazard to exist. For instance, if one or more hazard reports were received regarding the flight crew incorrectly selecting a switch (L-H), the SHEL model could be used to assist in understanding the circumstances that are causing the human error to be repeated. It might lead the investigation of the hazard to look at the checklist (L-H-S), or the application of the checklist in a two-pilot crew (L-L-S); or possibly the training (L-S); or even the installation of the switch – perhaps near a very similar switch – that is used during a busy sequence of tasks L-H-E).

The SHEL model may also be used to analyze the types of hazards that are being identified, perhaps with a certain aircraft type or a certain aspect of the operation. In such a circumstance, similar findings of L-L-S might suggest system-safety deficiencies in procedures or training.

The SHEL model may be useful when analyzing mitigation. For instance, if hazards in one part of the operation (e.g. flight ops rather than, say maintenance) are continuously mitigated by a re-writing of company operating procedures (L-L-S), and if the hazards reappear even after the changes in the procedures have been implemented, it might suggest that operational mitigation is not addressing the actual precipitating circumstances. If upon further examination the problem is identified as being related to the use of a certain aircraft type into a certain type of operating environment, it is probably an (L-H-E) interface that needs to be addressed.

Additional human factors information is contained in Appendix B.

## 6.4 Developing Mitigation

### 6.4.1 Steps in Developing Mitigation

Development of mitigation to either eliminate the hazards or reduce the associated risk to a level as low as reasonably practicable is a very important part of the hazard identification process. The first step is to focus on the event scenarios that have been identified as having the highest risk. As an extreme example, if you identified many hazards relating to the operation of a particular aircraft type at a specific site, then ceasing operation of that type of aircraft into the aerodrome might be warranted. Using the same example, if the most significant hazard was identified as marginal weather or night operations into the aerodrome at this site, then devising special conditions or restrictions for such operations might be appropriate.

- Focus on the event scenarios that have been identified as having the highest risk.
- Address key hazards embedded in the event scenarios.
- Mitigate to reduce the likelihood of the occurrence of events related to serious single hazards that have been identified.
- Mitigate the severity of the risks

The following form, which is also in the ***Hazard Identification Tools*** in the ***IBAC SMS Toolkit,*** may be used for developing mitigation.

| Hazard Sheet |
|---|
| **Hazard Statement:**<br><br>**Exposure (if applicable)** |
| **Event Scenarios (circle) 1 2 3 4 5 6 7 8** |
| **Mitigation:**<br><br>**Assumptions** |
| **Severity Category A B C D**<br><br>**Likelihood H M L R VR** |

Next, the team should address key hazards embedded in the event scenarios. To illustrate with another, unrelated example: if pilot fatigue was found to be a hazard that occurred in all scenarios that involved an extended duty-day and a return-flight segment after midnight, then a fatigue countermeasure program with limits on such operations might reduce the likelihood of fatigue occurring.

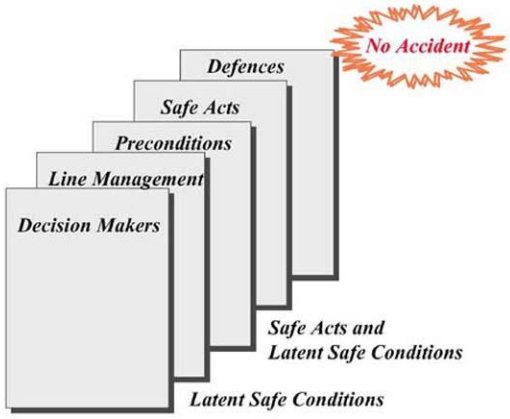
The team should next return to each event scenario and address the individual hazards they have identified. The goal is to reduce the likelihood of events occurring. However, it is important also to consider measures that reduce the consequences in the event an accident does occur. An example would be a procedure that consistently leads to a go-around rather than (even a low probability) of a collision with an obstacle. Let the information flow freely during this phase of developing mitigation. The ideas will subsequently be refined so that they are realistic and appropriate.

Mitigation may include:

- Procedure,
- Training,
- Equipment,
- Limitations or restrictions, or
- Any combination of the above.

Before turning from one event scenario to the next, ensure that the team is confident that the likelihood and severity of a serious accident has been reduced to a level that is as low as reasonably achievable. This normally means that there are a number of measures that collectively prevent a critical hazard from occurring, or if it does occur, from it leading to an accident, and if it does, from it leading to loss of life.

**Build Safety Layers**




### 6.4.2 Tips in Developing Mitigation

***Be aware of mitigation that might introduce new hazards or risks.***
Beware of mitigation that might introduce new hazards or risk to the operation. Examples could include new activities that introduce distractions during critical phases of the flight, or procedures that interfere with completing concurrent procedures.

***Mitigation must be realistic***
Not all mitigation is appropriate. For instance, it is not wise to expect consistent, error-free human performance as the sole way to prevent an accident. Challenge the team to determine whether the mitigation they are proposing is realistic given what they know about people, equipment and operations. If there is doubt, have them consider what can be done instead of, or in addition to, what they propose.

***Will the mitigation produce consistent results?***
Not all mitigation is effective. For instance, proposed mitigation may assume a degree of proficiency that is unrealistic to expect under all circumstances. In this case, supplementary mitigation may be necessary. Again, the team should be challenged to test whether the planned mitigation will always perform as well as they intend, or as the criticality of the hazard or hazards may require

***Address reduction to severity***
Remember to mitigate for severity when necessary. For instance, changes to flight watch procedures at hazardous, remote locations could improve search and rescue alerting services, thus reducing the likelihood of loss of life. Enhanced survival and first aid equipment coupled with a requirement for crews to be trained and proficient in the related skills could reduce the probability of a loss of life for survivors of an accident.

### 6.4.3 Assess the Mitigation

The next step is to assess the proposed mitigation by determining the likelihood and severity of accidents occurring after the mitigation has been implemented. This is important because:

- it enables the team to finalize their recommended actions to mitigate hazards and risks;
- it clearly documents for company executives, insurers, and the civil aviation authority what has been deemed to be acceptable risk; and
- it enables future reassessment of the hazards in the operation, and ongoing measurement of the appropriateness and effectiveness of the mitigation.

Criteria such as that presented in the Classification of Severity and Likelihood table in section 6.2.2 or Appendix C should be used when determining severity and likelihood.

It is customary to assess **severity** first and to consider worst-case scenarios. In other words, if one or more persons could foresee ably die during an event, then the severity should be categorized as a Category A. The subsequent assessment of likelihood will put the worst- case scenario into a realistic, operational context.

It is sometimes difficult to get agreement amongst your team on the **likelihood** of an accident occurring. In addition to the experience of the team members, draw on occurrence information from the databases of aircraft manufacturers, aviation associations and national and international safety agencies. It may be difficult to obtain early consensus regarding the likelihood of a single event, but after the team completes a few, overall consistency usually starts to emerge.

### 6.4.4 Refine the Mitigation

Once the likelihood and severity have been considered, review the mitigation that was previously suggested to verify that it is appropriate. It is important that a disproportionately high amount of resources not be expended to address hazards with a low probability of leading to an accident, at the expense of those more likely to occur.

| |
|---|
| Verify that the mitigation is appropriate to the likelihood and severity of the risk |

### 6.4.5 Documenting the Analysis

Always document a hazard identification and analysis, no matter what the scope of it is. The purpose of doing a hazard identification is to make good decisions. The process requires time to complete and sometimes money to mitigate the risks. Therefore, it is important that these investments of time and money yield a safety return. Without accurate documentation, it may not be possible to determine whether the risks are being well managed. Without accurate documentation, it is impossible to go back and measure the results of these investments in terms of achieving the safety performance objectives of the operation.

It may also be necessary to refer to the analysis should in the future there be a hazard identification report that cites an issue that may have been addressed in the earlier analysis. In such cases when reviewing the report and the original analysis try to determine the validity of the original analysis. During the review attempt to determine whether the hazard and associated risk were known and, if so, whether when the event occurred the implemented mitigation worked to prevent an accident or whether something unexpected happened and the mitigation must be revisited.

- Record the process, decisions and results
- Provide baseline for subsequent activities and analyses
- Avoid future duplication of effort

Without good documentation the risk of duplication of effort and “re-inventing the wheel” is significant.

One effective means of recording the results of the risk analysis and providing the information to those involved in the operation is to develop a safety-risk profile and to include it in the operations manual. Safety-risk profiles are discussed in section 9.2.

# 7. SAFETY ASSURANCE AND ONGOING SAFETY MANAGEMENT ACTIVITIES

## 7.1 Safety Performance Monitoring and Measurement

An SMS has a number of mechanisms that provide feedback on the effectiveness of safety management activities and hazards and risks that are being experienced. Safety performance monitoring and measurement activities should utilize things such as hazard reports, incident reports, committee meetings, and audit or inspection findings. In all cases, the information should be examined to determine the performance of the SMS and to identify indications of new and emerging hazards, ones that may have been missed in the original hazard analysis or any system safety deficiencies. In that process it may be useful to employ the SHEL model, discussed in section 6.3, to aid in the identification of hazards and system safety deficiencies. The information can then be tracked with other hazard-related information.

Operational processes and procedures should also be assessed at regular intervals to ensure that they are appropriate and effective. Other safety assurance activities that can help with that plus also help to ensure that identified problems have been resolved and that can assist in ensuring the efficiency of safety management activities is maximized, include:

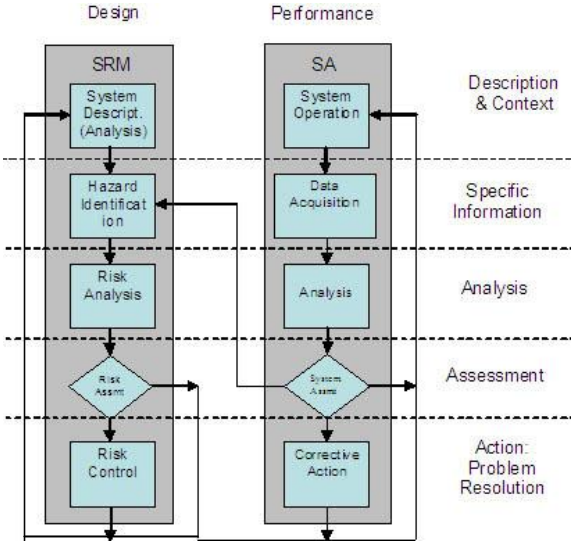
- Utilizing checklists tailored to the organization's operations when conducting safety evaluations,
- Assessing the activities of contractors where their services may affect the safety of the operation,
- Having assessments periodically reviewed by an independent source,
- Documenting safety assessment results and corrective actions,
- Documenting positive observations,
- Categorizing findings to assist in prioritizing corrective actions,
- Sharing the results and corrective actions with all personnel,
- Utilizing available technology such Flight Data Assessment to identify operational issues,
- Holding regular safety meetings,
- Keeping the owner/CEO/Accountable Executive informed of safety issues, and
- Investigating incidents and providing feedback to management and staff.

Regular evaluation of safety performance is an integral part of safety management system continuous improvement.

Evaluate to verify safety management activities are appropriate and effective and that safety performance expectations are being met.

Track evaluation results in a hazard identification and tracking system.

The relationship of Safety Assurance (SA) to Safety Risk Management (SRA) is shown the flowchart below. The flowchart depicts the input-output relationships between the activities in the processes. Significant aspects of these relationships are the interfaces between processes that 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.




The steps in the safety assurance process can be described as follows:

**System operation** – Monitoring and management of the risk controls will be one of the most important steps in safety assurance.

**Data acquisition** – Next, a variety of data is collected to test the controls. These data range from continuous monitoring (e.g. dispatch

procedures), to periodic auditing, to employee reporting systems that fill in the gaps. It also includes investigations to learn from our failures.

**Analysis** – Next the data is analyzed in relation to the SMS performance objectives and to determine the causes of any shortfalls. Also, be on the lookout for any new conditions that haven't seen before and unexpected results of system performance.

**System assessment** – The assessment process is where decisions are made. If the assessment results indicate that the SMS is performing appropriately, the checking, analyzing, and assessment processes continue so that the system performance is continuously confirmed.

**Corrective action** – If the desired results are not being achieved, corrective action in needed. This need not entail the same level of detail that was used in initial design. Many times, the corrective action needed is straightforward.

Sometimes, though, everyone is doing everything that was expected but it just isn't working to control the level of risk (possibly the conditions have changed so that the original control no longer is appropriate). This can be because of changes in contracts, changes to airports, new equipment, changing demographics of employee hiring pools or a variety of new conditions. In that case, a new and/or an uncontrolled hazard has been identified so it is necessary to revisit the risk management process to re-design the system aspects (e.g. new procedures, training, etc.) or develop new controls.

Further information on the safety assurance process can be found in the FAA SMS Assurance guide that is posted in the IBAC SMS Information Library at http://www.ibac.org/safety-management/sms-information-library.

In addition, information on SMS evaluation is contained in the ***SMS Evaluation Tool*** in the ***IBAC SMS Toolkit*** and information on internal audit is contained in the ***IS-BAO Internal Audit Manual*** on the IS-BAO CD.

## 7.2 Hazard Identification and Tracking System

One key element of the safety assurance process is the **hazard identification and tracking system** (HITS). It can be used to track the mitigations that have been implemented, in order to verify that they are appropriate and effective, and to identify emerging hazards or latent conditions that may have not been identified in the original hazard identification. There should be a form, paper or electronic or both, that operator personnel, passengers and others involved in the operation can use to record their observations and provide them to the manager or appointed person, to analyze, record their determination and provide feedback to the originator.

The format used should be compatible with the format of other information management systems that the operator uses. An example of a hazard identification and tracking tool is the ***HITS Tools*** in the ***IBAC SMS Toolkit***.

Regardless of the format used it must create a permanent record that can be readily accessed by management and used for periodic evaluation safety management performance.

- The HITS should be compatible with other operator information management systems.
- It should be used to create a permanent record that can be used to evaluate safety performance.

It is extremely important that a positive safety culture exists in the organization or employees may be hesitant to report safety concerns and errors including omission, slips, lapses, mistakes and violations they have committed.

It is also important so that sound feedback will be provided on the appropriateness and effectiveness of risk mitigation actions and related systems and procedures. It is through such feedback that safety management activities can be optimized to enhance the efficiency of the operation.

The attributes of a positive safety culture will be discussed in section 10.1 *Corporate Safety Culture*.

Safety concerns and errors must be

- Reported,
- Analyzed, and
- Addressed by appropriate mitigation that is developed, implemented and tracked.

The need for reporting of safety concerns and their subsequent analysis is obvious. The need for reporting of errors, including omission, slips, lapses, mistakes and violations, is equally important because these errors are most often indicators of latent conditions (system safety deficiencies). Therefore, it is essential that they be reported and analyzed and that mitigation be developed, implemented and then tracked to verify that it is appropriate and effective.

## 7.3 Using the HITS and Safety Assurance

When analyzing the HITS reports and other safety assurance information it is important to ensure that the embedded hazards and system safety deficiencies are identified and the associated risks are assessed. In other words, a symptom or a consequence must not be misidentified as the cause. Keep in mind the accident causation model that is described in section 3.1.3 and the risk analysis process discussed in section 6.2.

In the course of the analysis of HITS reports the records of the original hazard identification and subsequent risk analysis activities should be reviewed to ensure that time is not spent duplicating efforts.

As noted previously, it is important to determine if a report relates to an issue that may have been addressed in the earlier analysis. In such cases, when reviewing the report and the original analysis try to determine the validity of the original analysis. In the review, attempt to determine whether the hazard and associated risk were known and, if so, whether, when the event occurred, the implemented mitigation worked to prevent an accident or whether something unexpected happened and the mitigation must be reviewed.

When the analysis is completed provide feedback to the originator. It is also important that when the analysis is completed and the mitigation strategies are developed, information on them is made available to all of the personnel who may be exposed to the risk or who are involved in the application of the identified mitigations.

**Using the HITS**

- Analyze the HITS report,
- Review earlier analyses,
- Modify existing or develop new mitigation if required,
- Provide feedback to originator,
- Inform all personnel involved,
- Update safety-risk profile if required, and
- Conduct post-implementation review.

The identification of new hazards and safety-risks may also result in the need to update the Safety Risk Profile.

The safety-risk profile should also be modified when significant change in the operation is anticipated or experienced. In many cases, this will require revisions to all of the three sections of the profile.

When new mitigation is introduced or existing mitigation is modified, a post-implementation review should be conducted so as to ensure that the safety issue was correctly analyzed and that the mitigation is appropriate and effective.

## 7.4 Other Data Sources

. External safety data sources can be a useful supplement to internally generated data. For example, IBAC produces an annual *Business Aviation Safety Brief* that includes an analysis of the safety performance of business aviation worldwide. It is posted on the IBAC web site at http://www.ibac.org/safety-management/business-aviation-safety-brief.
Also, the Flight Safety Foundation and the various national and regional business aviation associations and regulatory agencies regularly publish safety information. Some of these sources are the Aviation Safety Network at http://aviation-safety.net/index.php and NASA's ASRS on-line data base at http://asrs.arc.nasa.gov/search/database.html.

Another information source available to business aircraft operators is flight data analysis programs, also known as flight operations quality assurance (FOQA) or flight data monitoring programs. Information on the UK CAA FDA/FDM programs can be found at http://www.caa.co.uk/default.aspx?catid=100 and the FAA Advisory Circular 120-82.

## 7.5 Risk Assessment as a Way of Life

There are many benefits that may be derived from flight department personnel using risk

assessments in day-to-day operations. Not only do risk assessments enhance safety, they also enhance operating efficiency and customer satisfaction.

Simple tools, such as the ***Risk Awareness Tool*** the ***IBAC SMS Toolkit*** that was developed by the Harley-Davidson flight department, have provided proven safety benefits.

Tools such as the ***Operational Risk Analysis Tool*** in the ***IBAC SMS Toolkit*** that was developed by T-Bird Aviation have been used in the trip-planning phase to enhance safety, operating efficiency and customer satisfaction.

## 7.6 The Management of Change

Aviation operations experience change due to expansion, contraction, changes to existing systems, equipment, programs, products and services, and introduction of new equipment or procedures. Hazards may inadvertently be introduced into an operation whenever change occurs. Effective safety management requires that hazards that are a by-product of change be systematically and proactively identified and that strategies to mitigate the safety-risks that are the consequences of hazards be developed, implemented and subsequently evaluated. Safety reviews and audits are also a valuable source of information and decision making under circumstances of change.

Change can impact the appropriateness of existing safety risk mitigation strategies, and/or impact the effectiveness of existing safety-risk mitigation strategies. Changes may be external to the organization, or internal. Examples of external changes include changes of regulatory requirements, changes in security requirements, and reorganization of air traffic management services. Examples of internal changes include management changes, new equipment and new procedures.

A management of change process should identify changes within the organization which may affect established processes, procedures, products and services. Prior to implementing such changes, the arrangements to ensure safety performance during the changes should be established and disseminated throughout the organization. The objective of this process is the reduction in the safety-risks resulting from the changes to a level as low as reasonably practical.

## 7.7 Accident and Incident Investigation

If an operator is unfortunate enough to suffer a major aircraft accident it will most probably be investigated by the national accident investigation authority. However, less serious accidents and incidents are indications that there may have been a failure in the defenses provided by the safety management system or that a defense many not have been appropriate or effective. Accidents and incidents should be investigated to identify the hazards and, in many cases, the system safety deficiencies that contributed to the failure in order to develop mitigation that will be appropriate and effective.

The investigative role may be assigned to persons who are trained accident investigators, if the operator is fortunate enough to have such people on staff. Other available resources may be corporate personnel who have such training or qualified consultants who can be retained for that purpose.

## 8. EMERGENCY RESPONSE PLANNING

While the foregoing proactive safety activities will reduce the likelihood of an incident or accident occurring, as was previously noted, in the aviation environment risk cannot be eliminated. Therefore, it is appropriate to devote some consideration to managing safety should an emergency occur or an accident happen.

An emergency response plan is one piece of the safety management system that operators hope that they will never have to use – but if it is ever needed, it has to be right. The emergency response plan should be designed to also maximize the possibility of continued survival of personnel involved in an accident. How an organization fares in the aftermath of an accident or other emergency can depend on how well it handles the first few hours and the days following a major safety event.

An emergency plan outlines in writing what should be done in the case of an emergency or after an accident, and who is responsible for each action.

To be able to respond successfully to an emergency, it is necessary to start with effective planning. An emergency response plan provides the basis for a systematic approach to managing the organization's affairs in the aftermath of a significant unplanned event — in the worst case, a major accident.

**Goals of an Emergency Response Plan**

1. Orderly and efficient transition from normal to emergency operations.
2. Delegation of emergency authority.
3. Assignment of emergency responsibilities.
4. Authorization by key personnel for actions contained in the plan.
5. Coordination of efforts to cope with the emergency, both initial response and ongoing activities.
6. Safe continuation of operations or a return to normal operations as soon as possible.

The suggested contents of an emergency plan are set out in the ***Emergency Response Plan Tool*** in the ***IBAC SMS Toolkit.***

Operators may obtain assistance in developing an emergency response plan through workshops held by the National Business Aviation Association (NBAA) or from specialty organizations. Also, see the European Business Aviation Association (EBAA) Emergency Response Guidance Manual.

It is very important to regularly exercise the emergency response plan so that those involved are fully conversant with their duties and to ensure the integrity of the plan.

The emergency response plan should be updated when there are changes in the organization or when deficiencies are identified.

Regularly exercise and update the emergency response plan.

# 9. DESIGNING THE SMS

## 9.1 Gap Analysis

The challenge to flight department management personnel will be how to design and implement a functional safety management system for their flight department in the most efficient and effective manner. Fortunately, most flight departments have many of the elements already in place, however, they may not be documented and linkages may be lacking. A tool that may be used for managing the SMS implementation is the ***SMS Gap Analysis Tool*** in the ***IBAC SMS Toolkit***.

**The tool is designed to:**

1. facilitate the process of ensuring that everyone involved has a common understanding of the purpose and scope of the SMS,
2. catalogue the existing policies, programs, systems and procedures that may meet the SMS elements performance requirements and identify the gaps that exist,
3. identify gaps where new policies, programs, systems and procedures are required, and
4. facilitate development of an SMS implementation plan.

The tool should help those involved to make maximum use of existing policies, programs, systems and procedures and to efficiently and effectively develop an SMS that is appropriate to the size and complexity of their operation. It also can be used in developing the SMS implementation plan.

As previously noted, it is recommended that senior management be engaged in the process at the start of the development of a safety management system so as to ensure that the required resources are provided and that ongoing safety management activities are fully supported.

While the **operational case** may be of interest to senior management they will most probably become engaged and supportive if the **business case** is well presented.

## 9.2 Safety-Risk Profile

### 9.2.1 Development Options

Before or during the gap analysis, there needs to be a determination of the key safety management issues that the company faces. This directly influences the design of the SMS. Some of the issues may be very specific to hazards encountered during specific elements of the operation. Others may relate to the challenges that have the potential to cause system safety deficiencies if not aggressively managed (e.g. fatigue management issues; the use of aircraft types that are not optimum for the company's operation; predictable resource-based issues, remote operations; etc.).

A company can use the hazard identification and analysis processes discussed earlier, or they may wish to do a high-level safety-risk profile of their operation and organization. In either case, a safety-risk profile will be developed to design the SMS. The profile is documented, and becomes a foundation for the SMS, which is updated periodically after the SMS is implemented.

The process involves the collection of data to identify safety hazards or latent unsafe conditions, so that associated risks can be assessed, mitigation introduced (or sustained) and a safety-risk profile developed. The data for this process may be derived from various parts of the operation.

**Obtain data from**

- The equipment used
- The people involved in the operation
- Work procedures
- The human/equipment/procedures interactions, etc.
- Industry data banks

In larger operations there may be management systems that can be accessed to assist in identifying safety hazards and latent unsafe conditions, and in assessing the associated risks. Data from these management systems should be used to the maximum extent practicable.

In most small flight operations there will not be much data available, however industry data can be used and, in any case, most of the people

involved in the operation will have information that can be used in the process.

### 9.2.2 Safety-Risk Profile Overview

A safety-risk profile is a documented overview of the safety risks that are generally experienced by an organization. It is like a map that charts the "contours" of highest risk and is the basis on which the safety management system is developed. The purpose of a safety-risk profile is to ensure that the resources expended on safety are appropriately targeted and will result in optimum safety performance. A safety-risk profile is unique to each operator. It is an explicit depiction of the hazards or types of hazards that are encountered in the flight operation, documented so that the related risks can be identified, assessed and managed. The safety-risk profile must be sufficiently well documented to permit corporate executives, auditors, insurance underwriters and other interested parties to understand how the safety risks of the operation have been identified, assessed and managed. A completed safety-risk profile will highlight and explain the areas of highest risk, justifying the need to effectively manage the risks. As such, it is an integral part of the safety management strategy that is discussed in section 9.3.2.

**Safety-Risk Profile**

- It is like a map that charts the "contours" of highest risk.
- It helps to ensure that resources expended are appropriately targeted.
- It helps users to understand safety management activities.

### 9.2.3 Simplified Process

While the initial hazard-analysis process does not need to be complex, it should be designed to reflect the size and complexity of the operation and can be adjusted to suit the time and resources available.

When the hazard-analysis is completed, the next step is to use the information from the hazard analysis to develop the safety-risk profile for the operation. Operators involved in implementation of the IS-BAO can use the ***Safety Risk Profile Tool*** in the ***IBAC SMS Toolkit*** or any similar format that they may choose.

### 9.2.4 Safety-Risk Profile Contents

The safety-risk profile normally contains the following information.

**A description of the operation**
The purpose of this brief section (one or two paragraphs) is to provide context for the description that follows of the medium- to high-risk elements of the company's flight operation. The contextual information can include

1. the number and types of aircraft operated by the company,
2. the approximate number of hours flown annually,
3. the number of persons associated with the flight operation, including their duties and qualifications,
4. representative passenger or cargo loads,
5. the routes or general geographic areas in which the operations are conducted,
6. the type of operations generally flown and the supporting infrastructure - IFR or VFR, the classes of airspace in which operations are normally conducted, dispatch or flight following procedures, access to weather and flight planning facilities, etc.,
7. maintenance and servicing facilities, and
8. anything else that describes the nature of the operation.

**A description of the significant hazards**
The description of the operation is followed by a description of the areas in which key or significant hazards have been identified in the operation. The purpose of this section is to present the basis and, therefore, the rationale, for the measures the company is taking to reduce the likelihood of an accident. The information is derived from the hazard-analysis and, particularly, from the information regarding the more probable or critical events and the more significant hazards to which the operation is exposed.

**A description of the mitigation**
It includes a general description of the measures used to mitigate the significant safety risks. This section will be the basis for the safety performance objectives and goals and the criteria by which the company's safety management system will be evaluated.

**Linkage to mitigation**
This section should reference the section where the detailed mitigation is located. Such mitigation could include training specifically intended to mitigate risks experienced by the operation, flight dispatch requirements, cabin safety requirements, etc.

**Keep it current**
It is also important to update the safety-risk profile when new hazards are identified, safety risks are reassessed, or significant change in the operation occurs.

## 9.3 Putting it All Together

### 9.3.1 Managing the Process

A significant amount of resources may have been expended in SMS development activities and, in order to gain the maximum possible benefits, the implementation of the SMS must be carefully managed. The ***SMS Gap Analysis Tool*** in the ***IBAC SMS Toolkit*** and the sample SMS development work plan presented in section 9.3.4 can be of great assistance in the implementation process.

An appropriate and effective implementation plan will ensure that:

1. management is informed and engaged in the process,
2. all flight department personnel involved in the operation are informed and engaged in the process,
3. individuals or committees that have been assigned responsibility for specific implementation tasks are identified and provided with the resources required to complete the tasks,
4. milestones have been identified so that the implementation efforts can be tracked and, if necessary, the resources assigned can be adjusted, and
5. linkages are maintained between all policies, programs, systems and procedures.

In a busy flight department or an air transport operation there will always be many pressures on resources and competing goals, so the importance of establishing realistic milestones and tracking them to verify that they are met cannot be over-emphasized.

The results of the gap analysis and the safety-risk profile are used to develop a plan to incorporate the identified mitigation into the appropriate systems, programs, procedures and manuals or other documents. Where the mitigation involves changes to operating procedures, operating manuals, training programs, etc., it may take a significant amount of effort and time to implement. Remember to stay focused on the reasons for building the safety management strategy, and not to be distracted or diverted by a few extra things that could be included to provide an additional buffer to a minor safety issue. Such activities can often result in an unwitting waste of safety resources. Remember that a good safety management system expends a company's resources (both time and money) appropriately and effectively to manage safety risks. In this way, the bottom line of the company is protected and resources are available to be applied to significant and emerging safety issues.

| Focus on appropriate and effective use of safety resources. |
|---|

### 9.3.2 Safety Management Strategy

A safety management strategy is the organization's approach to the management of safety. It is the linkage between the risks identified on the safety-risk profile and the remainder of the safety management system. It provides a summary explanation of, and rationale for, the safety management activities conducted by the operator. This document is the performance standard by which the regulatory agency, insurance underwriters, and others can evaluate safety performance. The safety management strategy normally contains the following:

1. a description of the nature of flight operations;
2. the safety-risk profile of the operator;
3. a list of the hazards and risks identified and the strategies adopted to mitigate them;
4. safety performance objectives that document the direction and activities being taken to enhance safety performance;
5. the mechanisms employed to monitor the flight department performance in relation to stated objectives and goals and to evaluate the effectiveness of the operator's safety management;
6. Linkage to the operator's safety assurance processes (see chapter 7); and

7. a description of other tools employed to manage the risks.

As the safety management strategy is being developed make sure that the linkages to the other components of the safety management system are being maintained.

| Maintain linkage between SMS components. |
|---|

An example of the material that may be contained in a safety management strategy is contained in the ***Safety Management Strategy Example*** in the ***IBAC SMS Toolkit***.

The safety management strategy should also include a means to identify all regulations, standards, exemptions, and guidelines applicable to the operation and to demonstrate compliance with them. In a non-commercial operation, this would include the national aviation regulations and, where applicable, the international rules or the rules of the specific country in which operations are conducted. In addition, for commercial operators, the regulatory requirements would include those related to their air operator certificate. A sample compliance monitoring checklist for a small operator is contained in the ***Compliance Monitoring Tool*** in the ***IBAC SMS Toolkit***.

| Include a system for identifying all regulations, standards, exemptions, and guidelines applicable to the operation and for demonstrating compliance with them. |
|---|

The mitigation implementation strategy and safety performance objectives should be developed in consultation with senior management and the accountable executive in order to ensure that they are committed to development of the safety management system and that the required resources, time and money, will be provided.

The mitigation implementation strategy should include incorporation of the mitigation that has been developed to manage the identified hazards and risks into the appropriate:

- systems,
- programs,
- procedures, and
- manuals or other documents.

In this process, it is important to maintain the linkage between hazards, associated risks and mitigation and to verify that the mitigation remains appropriate and effective.

At all times ensure that the scarce resources of people, time and money are used efficiently.

The mitigation implementation strategy should also identify the people who are responsible for related activities and their accountabilities within the safety management system. These accountabilities should also be reflected in the safety policy.

An example of an SMS development work plan is presented in section 9.3.4 as a means to track the development and implementation of a safety management system. The results of the gap-analysis should be used to modify the SMS to fit the specific requirements.

### 9.3.3 SMS Training and Education

It is recommended that an SMS education and training program be included as part of the SMS – when it is being implemented and later as it matures. The education and training program should cover the principles of safety and safety management, plus a briefing on, or discussion of, the specific elements of the company safety management system such as the safety-risk profile, the mitigation strategies, the hazard identification and tracking system and how they are to be used. As well as providing the training to current employees the training should be included in the company indoctrination training for new employees.

### 9.3.4 SMS Development Work Plan Example

| Action | Completion Date | | Comments |
|---|---|---|---|
| | Target | Actual | |
| **1. Study the SMS Concept** | | | |
| **2. Obtain Senior Management Commitment** | | | |
| 2.1 Agree to be involved and committed to SMS | | | |
| 2.2 Agree to draft policy, acceptable level of risk and strategic safety objective | | | |
| 2.3 Agree to provide required resources | | | |
| 2.4 Agree on accountabilities within the organization | | | |
| **3. Establish SMS Team** | | | |
| 3.1 Agree on team structure and duties and responsibilities of groups and individuals | | | |
| **4. Conduct Gap Analysis** | | | |
| 4.1 Determine what you have and what you need | | | |
| 4.2 Develop implementation plan | | | |
| **5. Conduct Hazards and Risk Assessment** | | | |
| 5.1 Identify hazards and associated risks | | | |
| 5.2 Assess risks and develop mitigation | | | |
| 5.3 Develop safety-risk profile | | | |
| **6. Develop Safety Management Strategy & Safety Assurance Processes** | | | |
| 6.1 Develop strategy to apply mitigation to appropriate programs, systems and procedures | | | |
| 6.2 Confirm acceptable level of risk and strategic safety objective | | | |
| 6.3 Develop safety performance objectives and goals and evaluation criteria | | | |
| 6.4 Adopt/adapt ongoing risk assessment tools and procedures | | | |
| 6.5 Develop safety assurance processes and associated checklists | | | |
| **7. Identify Safety Accountabilities of Managers and Staff** | | | |

| Action | Completion Date | | Comments |
|---|---|---|---|
| | Target | Actual | |
| 7.1 Revise the accountabilities developed in step 2.4 and amend as required | | | |
| 7.2 Ensure accountabilities are reflected in organization charts, position descriptions, organization and other related manuals and documents | | | |
| 7.3 Assess and address any identified cultural issues to ensure a positive safety culture in the organization | | | |
| **8. Develop Hazard Identification and Tracking System and Risk Assessment Procedures** | | | |
| 8.1 Adopt/adapt forms and develop procedures for employees to provide feedback on mitigation and to report hazards and incidents | | | |
| 8.2 Adopt/adapt analysis procedures | | | |
| 8.3 Develop a risk register or similar system to track reports, analysis and rectification actions | | | |
| 8.4 Establish committees if they are being used | | | |
| 8.5 Set-up flight data analysis system if it is being used | | | |
| 8.6 Develop and implement ongoing risk assessment tools including the management of change | | | |
| **9. Develop Emergency Preparedness Plan** | | | |
| 9.1 Develop the ERP | | | |
| 9.2 Train those involved in the ERP | | | |
| 9.3 Exercise the ERP | | | |
| **10. Amend Programs, Systems and Procedures and Related Documents.** | | | |
| 10.1 Review previous activities and develop a list of programs, systems and procedures and related documents that require amending | | | |
| 10.2 Amend documents including the operations manual, as required | | | |
| 10.3 Ensure mitigation activities are integrated into programs, | | | |

| Action | Completion Date | | Comments |
|---|---|---|---|
| | Target | Actual | |
| systems, procedures and related documents | | | |
| 10.4 Ensure system is in place to demonstrate compliance with applicable laws, regulations, approvals, etc. | | | |
| **11. Train Staff** | | | |
| 11.1 Train staff to understand SMS principles and their role and responsibilities in the SMS | | | |
| 11.2 Ensure all staff members understand the hazards and risk involved in their segment of the operation and the mitigation being applied | | | |
| **12. Track and Evaluate** | | | |
| 12.1 Develop tools to evaluate the SMS and verify that the acceptable level of risk, the SMS safety objectives, goals and expectation are being met | | | |
| 12.2 Develop tools to track deficiency-rectification activities and to evaluate their appropriateness and effectiveness | | | |
| 12.3 Develop management review process that ensures that senior management is fully engaged in evaluation of the SMS and related safety management activities | | | |

# 10. BUILDING A SAFETY CULTURE

## 10.1 The Role of Culture in an SMS

Culture influences the values, beliefs and behaviors that we share with the other members of our various social groups. Culture serves to bind us together as members of groups and to provide clues as to how to behave in both normal and unusual situations. Some people see culture as the collective programming of the mind. Culture is the complex social dynamic that sets the rules of behavior, or the framework for all our interpersonal interactions. It is the sum of the way people conduct their affairs in a particular social environment. Culture provides a context in which things happen. For safety management, understanding the context provided by culture is important to the understanding of human and corporate performance. It is also important to the understanding of human and corporate strengths and limitations. For the safety management system to operate efficiently and effectively, it is important that it be supported by a positive safety culture.

**Culture**

- The values beliefs and behaviors of the group
- The collective programming of the mind
- How we do things here
- What is acceptable and what is not acceptable

The Western world's approach to management is often based on an emotionally detached rationality, which is considered to be "scientifically" based. It assumes that human cultures in the workplace resemble the laws of physics and engineering, which are universal in application. This assumption reflects a Western cultural bias, and an unrealistic expectation of human beings.

Aviation safety must transcend national boundaries, including all the cultures therein. On a global scale, the aviation industry has achieved a remarkable level of standardization across aircraft types, countries and peoples. Nevertheless, it is not difficult to detect differences in how people respond in similar situations. As people in the industry interact (the "Liveware-Liveware" interface), their trans-actions are affected by the differences in their cultural backgrounds. Different cultures have different ways of dealing with common problems.

## 10.2 Levels of Culture

Organizations also have a culture of their own. Organizational behavior is subject to these influences at every level. The following three levels of culture have relevance to safety management initiatives.

**National culture** recognizes and identifies the national characteristics and value systems of particular nations. People of different nationalities differ, for example, in their response to authority, how they deal with uncertainty and ambiguity, and how they express their individuality. They are not all attuned to the collective needs of the group, team or organization in the same way. In some cultures, there is acceptance of unequal status and deference to leaders. Such factors may affect the willingness of individuals to question decisions or actions. This is an important consideration in crew resource management. Situations where assignments mix national cultures may affect team performance by creating misunderstandings.

Similar circumstances may also be encountered in a range of situations when operations are conducted in foreign countries.

**National culture** recognizes and identifies the national characteristics and value systems of particular nations.

**Professional culture** recognizes and identifies the behavior and characteristics of particular professional groups such as the typical behavior of pilots vis-à-vis that of aircraft maintenance personnel or other professional groups. Through personnel selection, education and training, on-the-job experience, etc., professionals such as doctors, lawyers, pilots and aircraft maintenance personnel tend to adopt the value system of, and develop behavior patterns consistent with, their peers; they learn to "walk and talk" alike. They generally share a pride in their profession and are motivated to excel in it. On the other hand, they may have a sense of personal invulnerability. That is, they feel that their performance is not affected by personal problems and that they do not make errors in situations of high stress.

**Professional culture** recognizes and identifies the behavior and characteristics of particular professional groups.

**Organizational culture** recognizes and identifies the behavior and values of particular organizations. This is the behavior of members of one company compared with those of another company, or government versus private sector behavior. Organizations provide a shell for national and professional cultures. In an airline, for example, pilots may come from different professional backgrounds such as military versus civilian experience, and bush or commuter operations versus a large carrier. They may also come from different organizational cultures due to corporate mergers or layoffs. Generally, personnel in the aviation industry enjoy a sense of belonging. They are influenced in their day-to-day behavior by the values of their organization.

**Organizational culture** recognizes and identifies the behavior and values of particular organizations.

These values of the organizations may influence a number of factors, such as whether the organization:

- recognizes merit,
- promotes individual initiative,
- encourages risk-taking,
- tolerates breaches of SOPs, and
- promotes open two-way communications.

The organizational culture is a major determinant of employee behavior and has the greatest scope for creating and nourishing a culture of safety at the organizational level.

**Organizational sub-cultures** often exist if a subordinate group cannot tolerate the conditions imposed by the organizational culture. This is easier to imagine in a large operation, but even very small flight operations can experience a disparity between the culture espoused by an overbearing manager and that actually experienced by those reporting to the manager.

If a sub-culture exists, particularly within a small operation, it almost always negatively affects the safety culture.

## 10.3 Corporate Safety Culture

Corporate safety culture reflects the atmosphere created by management that shapes the attitudes about safety amongst personnel from the flight and maintenance departments. The safety culture is affected by factors such as:

- management's actions and priorities,
- policies and procedures,
- supervisory practices,
- safety planning and goals,
- actions in response to unsafe behaviors,
- employee training and motivation, and
- employee involvement or "buy-in".

It should be remembered: safety culture is never neutral. It is either positive, or it is negative. It always influences the function of the SMS, and the company's safety performance. A positive safety culture must be generated from the top down. It starts with the corporate safety policy and is built on the principles and actions of management.

Some of the attributes of a positive safety culture are described below:[1]

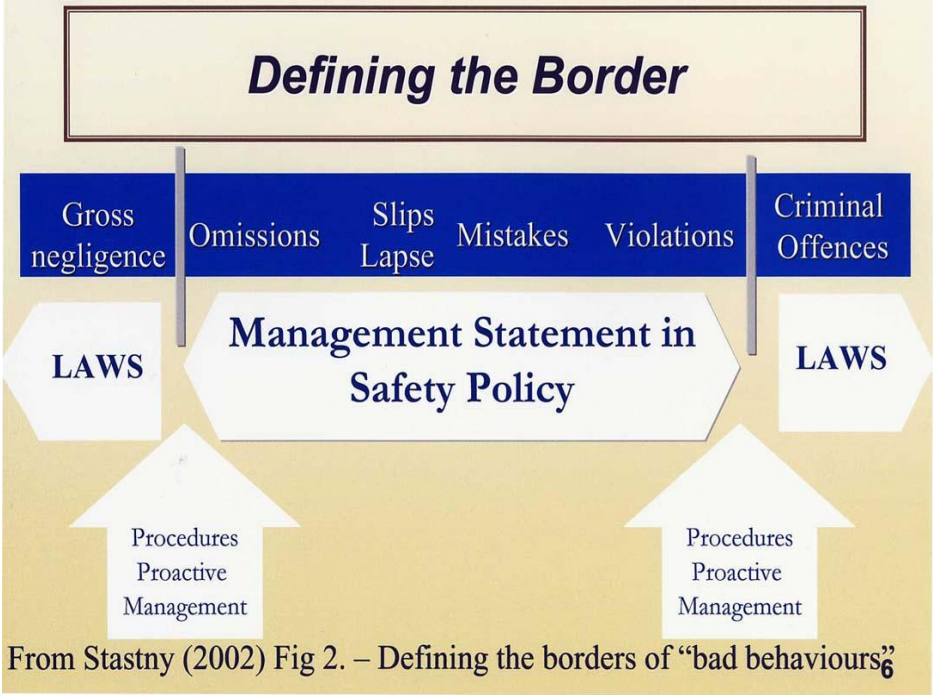
**An Informed culture:** Management fosters a culture where people understand the hazards and risks inherent in their areas of operation. Personnel are provided with the necessary knowledge, skills and job experience to work safely, and they are encouraged to identify the threats to their safety and to seek the changes necessary to overcome them. As a consequence, managers make better-informed decisions and have ongoing feedback.

**A Learning culture:** Learning is seen as more than a requirement for initial skills training; rather it is valued as a lifetime process. People are encouraged to develop and apply their own skills and knowledge to enhance organizational safety. Staff members are updated on safety issues by management and safety reports are fed back to staff so that everyone can learn the pertinent safety lessons. Learning progresses from individual managers and staff to the organization, which in turn feeds the "informed culture".

[1] Doc 9859 Safety Management Manual, ICAO Montreal.

**A Reporting culture:** Managers and operational personnel freely share critical safety information without the threat of punitive action. This is frequently referred to as creating a corporate reporting culture. Personnel are able to report hazards or safety concerns as they become aware of them, without fear of sanction or embarrassment.

**A Just culture:** An environment where staff members will report hazards, safety concerns and errors is fundamental for a good reporting culture. To achieve this it is important that the workforce knows and agrees on what is acceptable and what is unacceptable behavior. While it is recognized that slips, lapses, mistakes and violations may occur and the associated circumstances need to be addressed in a non-punitive manner, it is understood that gross negligence or serious offences are not and cannot be tolerated. A just culture recognizes that, in certain circum-stances, there may be need for punitive action. Therefore, it is important to define the line between acceptable and unacceptable actions or activities, and articulate this in the company's SMS. The following diagram provides a depiction of this environment.



From Stastny (2002) Fig 2. – Defining the borders of "bad behaviours"[6]

**Indications of a Positive Safety Culture**

1. Senior management places strong emphasis on safety as part of the strategy of control-ling risks including minimizing losses.
2. Decision-makers and operational personnel hold a realistic view of the short- and long-term hazards involved in the organization's activities.
3. Those in senior positions
   a. foster a climate in which there is a positive attitude towards criticisms, comments and feedback from lower levels of the organization on safety matters,
   b. do not use their influence to force their views on subordinates, and
   c. implement measures to contain the consequences of identified safety deficiencies.
4. Senior management promotes a just culture. As noted above, the term non-punitive **does not** imply blanket immunity.
5. There is an awareness of the importance of communicating relevant safety information at all levels of the organization (both internally and with outside entities).
6. There are realistic and workable rules relating to hazards, safety and potential sources of damage.
7. Personnel are well trained and understand the consequences of unsafe acts.

8. There is a low incidence of risk-taking behavior and a safety ethic that discourages such behavior.

For more information in Just Culture see http://flightsafety.org/files/just_culture.pdf and http://www.justculture.org/.

## 10.4 Assessing and Improving Your Safety Culture

The *Safety Culture discussion papers* by Dr. Don Arndt provide basic information on observing, testing and managing culture in an organization.

The *Safety Culture survey* tool by Dr James Reason, the Safety Culture Characteristics grid and the tools provided by Culture Dynamics can be used to assess the safety culture of an organization. If there are indications that there is room for improvement of the safety culture more detailed assessments can be performed by experts in the field to assess issues and provide a path to a congruent safety culture.

For additional information on resources available to assist with cultural assessment and developing a positive safety culture see the following web sites:

- *Cultural Dynamics*,
- *Human Engineering Consultancy*, and
- *The Just Culture Community*.

# 11. MANAGING SMS PERFORMANCE AND IMPROVEMENT

As with any activity that involves the expenditure of resources, regular evaluation of performance is an integral component of managing the activity. Some information on the appropriateness and effectiveness of the operator's safety management system may be gathered through informal feedback, some safety performance monitoring and measurement activities, HITS reports and discussion of safety management activities in regular or special safety meetings. While this is valuable information and may be used in the continuous improvement of the SMS, there should also be periodic evaluation in relation to stated safety performance objectives and goals to verify that safety management activities are appropriate and effective and that expectation are being met.

Safety performance objectives were discussed in section 5.3. The periodic evaluation of performance in relation to those objectives and goals should be recorded in a risk management tracking system. An example of a risk management tracking form that may be used is contained in the ***HITS Tools*** in the **IBAC SMS Toolkit.**

Information on SMS evaluation is contained in the ***SMS Evaluation Tool*** in the ***IBAC SMS Toolkit***.

Regular evaluation of safety performance is an integral part of safety management system continuous improvement.

Evaluate to verify safety management activities are appropriate and effective and that expectations are being met.

Track evaluation results in a hazard identification and tracking system.

The SMS evaluation process should include regular external audits. Operators who wish to achieve IS-BAO registration are required to undergo periodic audits by an accredited IS-BAO auditor. The certification and safety oversight audits of operators who hold an air operator certificate will probably include an audit of the operator's safety management system.

All SMS evaluation activities should include senior management review of the results of safety management activities, risk management results, lessons learned and SMS improvement opportunities. This will help to ensure that senior management is fully engaged in the SMS and safety management activities.

The end result of these efforts should be a safety management system that will ensure that safety is a core value of the organization and that safety is integrated into all management systems, including operational, maintenance, financial and human resource management, thereby enhancing the safety, efficiency and effectiveness of the operation.

## Glossary of Terms

| Glossary Term | Definition |
|---|---|
| Acceptable level of risk | The risk tolerance or safety expectations of an operator, or service provider, and their stakeholders and customers or an agency involved in safety oversight. |
| Accountabilities | The sum of duties and responsibilities assigned to personnel. |
| Active failures | Errors (slips, lapses or violations) that are committed by operators, either knowingly or unknowingly. |
| ALARP | An acronym used to describe a risk that has been reduced to a level that is *as low as reasonably practical*. |
| Culture | The values and beliefs of a group. |
| Defenses | Technical systems, or procedures and processes that are built into a system to protect the organization against inappropriate performance, poor decisions or other threats to the safety of the system. |
| Emergency response plan | A document that describes the actions that should be taken in the event of an emergency or accident. Such a document also identifies the person or entity that is responsible for each action. |
| Fully acceptable risks | Risks that are so low that they are fully acceptable to an organization. |
| Gap-analysis tool | A tool that provides a structured process to identify gaps between existing policies, programs, systems and procedures and the requirements of a safety management system. |
| Hazard | A condition or circumstance that can possibly lead to physical injury or damage. |
| Hazard analysis | The systematic process of identifying potential hazards, determining associated risks and developing mitigation strategies. |
| Hazard identification and tracking system (HITS) | An element of the SMS feedback process that can be used to track the mitigation activities that have been implemented in the operation. The HITS can also be used to identify and record information about new and emerging hazards. |
| Incident | An occurrence, other than an accident, associated with the operation of an aircraft that affects or could affect the safety of the operation. |
| Lapse | A failure of memory, such as when we either forget what we had planned to do, or omit an item in a planned sequence of actions. |
| Latent conditions | The inevitable characteristics of decision making by governments, regulators, system designers, manufacturers and organizational and operational managers that permit the circumstances where active failures and other hazards can exist. |
| Mitigation | Measures taken to eliminate a hazard or to reduce the likelihood or severity of a risk. |

| | |
|---|---|
| Mitigation implementation strategy | A plan to incorporate mitigation activities into the appropriate systems, programs, procedures, manuals and other documents in order to address hazards and risks identified by an organization. |
| National culture | The values and beliefs of people belonging to a particular nation. |
| Organizational culture | The values and beliefs of people belonging to a particular organization. |
| Positive safety culture | The culture within an organization that encourages continuously obtaining, learning from and using information to reduce safety-risks, so that everyone is enthusiastic and effectively engaged in improving the company's safety performance. |
| Preconditions | The assumptions about human and technical performance and the operational conditions in which aviation service are provided. These form the basis for most standards. |
| Professional culture | The values and beliefs of particular professional groups such as pilots, aircraft maintenance personnel, air traffic controllers, etc. |
| Risk | The consequence of a hazard, measured in terms of likelihood and severity. |
| Risk Management | A process to identify hazards and take reasonable measures to reduce risk to personnel, equipment and the operation. |
| Runway incursion | Any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle or person on the protected area of a surface designated for the landing and take-off of aircraft. |
| Safety | The state in which the risk of harm to persons or damage to property is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management. |
| Safety management strategy | An organization's approach to managing safety. It forms the link between the risks identified in the safety-risk profile and the remainder of the safety management system. |
| Safety Management System (SMS) - IS-BAO definition | The systematic and comprehensive process for the proactive management of safety-risks that integrates the management of operations and technical systems with financial and human resource management. |
| Safety Management System (SMS) - ICAO definition | A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures. |
| Safety policy | A high-level statement that details the desired corporate safety performance of an operation. It forms a link between the short-term goals, long-term safety objectives and the safety performance objectives of the organization. |
| Safety-risk profile | A documented overview of the safety risks that are generally experienced by an organization. |
| SHEL model | A model that can be used to depict the interrelationships among the various components in the aviation system. This model is an enhanced version of the traditional man-machine-environment system. |

| | |
|---|---|
| Slip | An action that was not carried out as planned. |
| Strategic safety objective | The safety performance expectations, of an operator, a service provider or an agency involved in safety oversight. |
| System safety deficiency | A circumstance that permits hazards of a like nature to exist. |
| Tolerable risks | Risks that meet the predetermined criteria that have been defined as acceptable to the organization. |
| Unacceptable risks | Risks that do not meet predetermined acceptability criteria. |
| Unsafe acts | The errors, slips and lapses and violations committed by aviation personnel in the course of their duties. |

## Further Information


Australian Government Civil Aviation Safety Authority, Canberra. *Advisory Circular 172-01(0) September 2005 Guidelines for Preparing a Safety Management System (SMS)* at http://www.casa.gov.au/wcmswr/_assets/main/rules/1998casr/172/172c01.pdf.

Australian Government Civil Aviation Safety Authority, Canberra. Various safety management documents at. *http://www.casa.gov.au/sms/toolkit/index.htm*

Australian Government Civil Aviation Safety Authority, *Safety Management Systems - An Aviation Business Guide*. CASA, Canberra.

Federal Aviation Administration, Washington. *Advisory Circular 120-92A Introduction to Safety Management Systems for Air Operators* at http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/0/678110F11B8433728625777D0068D732?OpenDocument&Highlight=120-92a

Federal Aviation Administration, Washington. *Flight Risk Assessment Tool* at http://www.faa.gov/other_visit/aviation_industry/airline_operators/airline_safety/info/all_infos/media/2007/inFO07015.pdf.

Flight Safety Foundation, Arlington. Various safety management documents at http://www.flightsafety.org/home.html.

GAIN Working Group E. *A Roadmap to a Just Culture – Enhancing the Safety Environment* at http://flightsafety.org/files/just_culture.pdf

Global Aviation Information Network, Arlington. Various safety management documents at http://flightsafety.org/archives-and-resources/global-aviation-safety-network-gain

International Civil Aviation Organization, Montreal. (1993) *Human Factors Digest No. 10*: *Human Factors, Management and Organization.* ICAO, Montreal.

International Civil Aviation Organization, Montreal. Doc 9859 *ICAO Safety Management Manual* at *http://www.icao.int/anb/safetymanagement/*

Reason, James. (1990) *Human Error. Cambridge, Cambridge University Press.*

Reason, James. (1997) *Managing the Risks of Organizational Accidents.* Aldershot: Ashgate

Reason, James. and Hobbs, Allan (2003) *Managing Maintenance Error – A Practical Guide*. Aldershot: Ashgate

The Air Line Pilots Association, *International. Background and Fundamentals of the Safety Management System (SMS) for Aviation Operations* at https://crewroom.alpa.org/safety/Default.aspx?tabid=2568

Transport Canada Civil Aviation. Various safety management documents at: http://www.tc.gc.ca/eng/civilaviation/standards/sms-menu-618.htm

Transport Canada. (2001) *Safety Management Systems.* (TP 13739) Ottawa: Public Works and Government Services.

United Kingdom Civil Aviation Authority London. *Safety Management Systems – Guidance to Organizations Operations* at http://www.caa.co.uk/docs/1196/20081010SafetyManagementSystems.pdf.

Wood, Richard H. (1991) Aviation *Safety Programs: A Management Handbook*. Englewood, Colorado. Jeppesen Sandersen Inc.

## Appendix A - ICAO SMS Components and Elements

# FRAMEWORK FOR SAFETY MANAGEMENT SYSTEMS (SMS)[2]

This appendix specifies a framework for the implementation and maintenance of a safety management system (SMS) by an organization. An SMS is a management system for the management of safety by an organization. The framework includes four components and twelve elements representing the minimum requirements for SMS implementation. The implementation of the framework shall be commensurate with the size of the organization and the complexity of the services provided. This appendix also includes a brief description of each element of the framework.

**1. Safety Policy and Objectives**

- 1.1 - Management commitment and responsibility
- 1.2 - Safety accountabilities
- 1.3 - Appointment of key safety personnel
- 1.4 - Coordination of emergency response planning
- 1.5 - SMS documentation

**2. Safety Risk Management**

- 2.1 – Hazard identification
- 2.2 – Safety risk assessment and mitigation

**3. Safety Assurance**

- 3.1 – Safety performance monitoring and measurement
- 3.2 – The management of change
- 3.3 – Continuous improvement of the SMS

**4. Safety Promotion**

- 4.1 – Training and education
- 4.2 – Safety communication

## 1. Safety Policy and Objectives

### 1.1 - Management commitment and responsibility

The organization shall define the organization's safety policy, which shall be in accordance with international and national requirements, and which shall be signed by the accountable executive of the organization. The safety policy shall: reflect organizational commitments regarding safety; include a clear statement about the provision of the necessary resources for the implementation of the safety policy; and be communicated, with visible endorsement, throughout the organization.

The safety policy shall: include the safety reporting procedures; clearly indicate which types of operational behaviours are unacceptable, and include the conditions under which exemption from disciplinary action would be applicable. The safety policy shall be periodically reviewed to ensure it remains relevant and appropriate to the organization.

### 1.2 Safety accountabilities

The organization shall identify the accountable executive who, irrespective if other functions, has ultimate responsibility and accountability, on behalf of the organization, for the implementation and maintenance of the SMS. The organization shall also identify the accountabilities of all members of management,

[2] Air Navigation Commission SMS Working Paper, ICAO, Montreal, 2008

irrespective of other functions, as well as of employees, with respect to safety performance of the SMS. Safety responsibilities, accountabilities and authorities shall be documented and communicated throughout the organization and shall include a definition of the levels of management with authority to make decisions regarding safety risk tolerability.

### 1.3 Appointment of key safety personnel

The organization shall identify a safety manager to be the responsible individual and focal point for implementation and maintenance of an effective SMS.

### 1.4 Coordination of emergency response planning

The organization shall ensure that an emergency response plan that provides for the orderly and efficient transition from normal to emergency operations, and the return to normal operations, is properly coordinated with the emergency response plans of those organizations it must interface with during the provision of its services.

### 1.5 SMS documentation

The organization shall develop an SMS implementation plan, endorsed by senior management of the organization, that defines the organization's approach to the management of safety in a manner that meets the organization's safety objectives and maintain SMS documentation to describe the safety policy and objectives, the SMS requirements, the SMS processes and procedures, the accountabilities, responsibilities and authorities for processes and procedures, and the SMS outputs. Also as part of the SMS documentation, the organization shall develop and maintain a safety management system manual (SMSM), to communicate its approach to the management of safety throughout the organization.

## 2. Safety Risk Management

### 2.1 Hazard identification

The organization shall develop and maintain a formal process that ensures that hazards in operations are identified. Hazard identification shall be based on a combination of reactive, proactive and predictive methods of safety data collection.

### 2.2 Safety risk assessment and mitigation

The organization shall develop and maintain a formal process that ensures analysis, assessment and control of the safety risks in operations.

## 3. Safety Assurance

### 3.1 Safety performance monitoring and measurement

The organization shall develop and maintain the means to verify the safety performance of the organization and to validate the effectiveness of safety risks controls. The safety performance of the organization shall be verified in reference to the safety performance indicators and safety performance objectives of the SMS.

### 3.2 The management of change

The organization shall develop and maintain a formal process: to identify changes within the organization which may affect established processes and services; to describe the arrangements to ensure safety performance before implementing changes; and to eliminate or modify safety risk controls that are no longer needed or effective due to changes in the operational environment.

### 3.3 Continuous improvement of the SMS

The organization shall develop and maintain a formal process to identify the causes of sub-standard performance of the SMS, determine the implications of sub-standard performance of the SMS in operations, and eliminate or mitigate such causes.

## 4. Safety Promotion

### 4.1 Training and education

The organization shall develop and maintain a safety training programme that ensures that personnel are trained and competent to perform their SMS related duties. The scope of the safety training shall be appropriate to each individual's involvement in the SMS.

### 4.2 Safety communication

The organization shall develop and maintain formal means for safety communication that ensures that all personnel are fully aware of the SMS; conveys safety critical information; and explains why particular safety actions are taken and why safety procedures are introduced or changed.

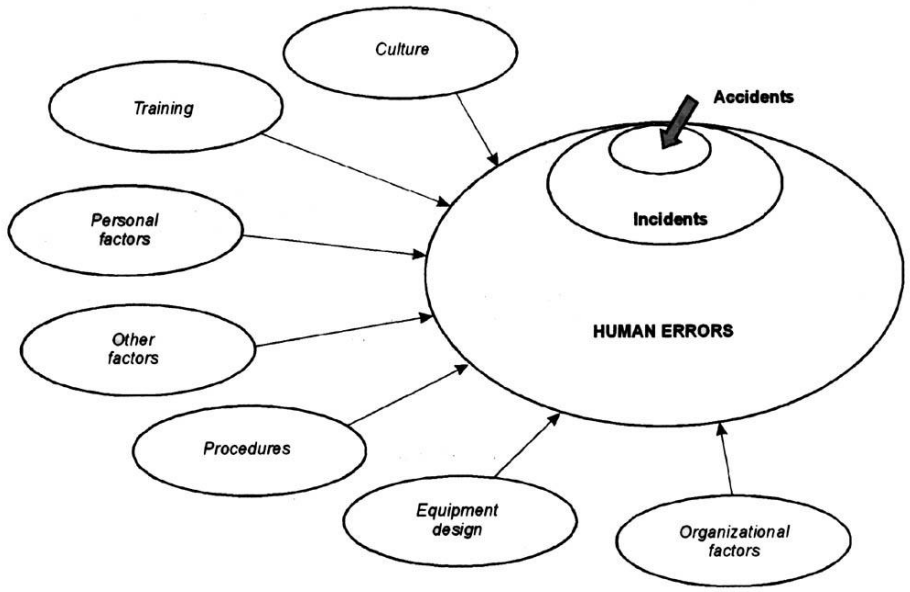
## Appendix B - Human Error Considerations

Adapted from Doc 9859 Safety Management Manual, ICAO, Montreal

### 1. Human Error

As previously noted human error is cited as a causal or contributing factor in the majority of aviation occurrences. All too often competent personnel commit errors, although clearly they did not plan to have an accident. Errors are not some type of aberrant behavior; they are a natural by-product of virtually all human endeavors. Error must be accepted as a normal component of any system where humans and technology interact. “To err is human.” To deal with human error is “management” – safety management!

**Factors contributing to human error**




Errors are not some type of aberrant behavior; they are a natural by-product of virtually all human endeavors.

The accident causation factors previously discussed describe the context in which humans commit errors. Given the rough interfaces of the aviation system as depicted in the “SHEL” model, the scope for human errors in aviation is enormous. Understanding how “normal” people commit errors is fundamental to safety management. Only then can effective measures be implemented to minimize the occurrence and effects of human errors on safety.

Even if not altogether avoidable, human errors are “manageable” through the application of improved technology, relevant training, and appropriate regulations and procedures. Most measures aimed at error management involve front-line personnel. However, the performance of pilots, aircraft maintenance personnel and other people in the operation are strongly influenced by organizational, regulatory, cultural and environmental factors affecting the workplace. For example, organizational processes constitute the breeding grounds for many predictable human errors, including inadequate communication facilities, ambiguous procedures, unsatisfactory scheduling, insufficient resources, and unrealistic budgeting - in fact, all processes that the organization can control.

### 2. Types of Errors

Errors may occur at the planning stage or during the execution of the plan. **Planning errors** lead to **mistakes**; either the person follows an inappropriate procedure for dealing with a routine problem or builds a plan for an inappropriate course of action to cope with a new situation. Even when the planned action is

appropriate, errors may occur in the execution of the plan.

When a person does not have a ready-made solution based on previous experience or training, that person draws on personal knowledge and experience. Developing a solution to a problem using this method will inevitably take longer than applying a rule-based solution, as it requires reasoning based on knowledge of basic principles. Mistakes can occur because of a lack of knowledge or because of faulty reasoning. The application of knowledge-based reasoning to a problem will be particularly difficult in circumstances where the individuals are busy, as their attention is likely to be diverted from the reasoning process to deal with other issues. The probability of a mistake occurring becomes greater in such circumstances.

Mistakes also occur due to misapplication of good rules or the application of bad rules.

**Planning errors** – mistakes
- Decisions "on the fly"
- Lack of knowledge or faulty reasoning
- Misapplication of good rules
- Application of bad rules

### 3. Execution Errors – slips and lapses

The human factors literature on such errors in execution generally draws a distinction between slips and lapses. A **slip** is an action that is not carried out as planned and will therefore always be observable. A **lapse** is a failure of memory and may not necessarily be evident to anyone other than the person who experienced the lapse.

**Slip**
- An action which is not carried out as planned
- Will be evident

**Lapse**
- A failure of memory
- May not necessarily be evident

The actions of experienced and competent personnel tend to be routine and highly practiced. They are carried out in a largely automatic fashion, except for occasional checks on progress. Slips and lapses can occur in several manners.

**Attentional slips** occur as the result of a failure to monitor the progress of a routine action at some critical point. They are particularly likely when the planned course of action is similar, but not identical, to a routinely-used procedure. If attention is allowed to wander or a distraction occurs at the critical point where the action differs from the usual procedure, the result can be that the operator will follow the usual procedure rather than the one intended in this instance.

**Attentional slip** - failure to monitor the progress of a routine action

Memory lapses occur when we either forget what we had planned to do or omit an item in a planned sequence of actions.

**Memory lapse** – forgot or omitted a planned action

### 4. Perceptual Errors

Perceptual errors are errors in recognition. They occur when we believe we saw or heard something that is different from the information actually presented.

**Perceptual Error** - Difference in what we really saw versus what we thought we saw.

### 5. Violations

Errors, which are a normal human activity, are quite distinct from violations. However both can lead to a failure of the system and both can result in a hazardous situation. The difference in errors and violations lies in the intent. A violation in this context is a deliberate act, while an error is unintentional.

**Violation -** Deliberate act contrary to a procedure, or a "work around"

Some violations are the result of poor or unrealistic procedures where people have developed "work arounds" to accomplish the task. In such cases, it is very important that they be reported as soon as they are encountered in order that the procedures can be corrected. In any event, violations should not be tolerated.

There have been accidents where a corporate culture that tolerated or, in some cases, encouraged the taking of short-cuts rather than the following of published procedures was identified as a contributory cause.

### 6. Error Management

Fortunately, few errors lead to adverse consequences, let alone accidents. Typically, errors are identified and corrected with no undesirable outcomes. On the understanding that errors are normal in human behaviors, the total elimination of human error would be an unrealistic goal. The challenge then is not merely to prevent errors but to learn to safely manage the inevitable errors.

**Error management** is an important part of safety management

Strategies for error management include **error reduction**, **error capturing** and **error tolerance**. Error reduction strategies intervene directly at the source of the error by reducing or eliminating the contributing factors that trigger the error.

**Error reduction** - reduce or eliminate the contributing factors

**Error capturing** assumes the error has already been made. The intent is to "capture" the error before any adverse consequences of the error are felt. Error capturing is different from error reduction in that it does not directly serve to reduce or eliminate the error, just to manage its consequence.

**Error capturing – "**capture" the error before any adverse consequences of the error are felt

**Error tolerance** refers to the ability of a system to accept an error without serious consequence.

**Error tolerance** – system ability to accept error

## Appendix C - Other Risk Categorization Systems

### Table 1: Measure of Risk Consequence and Likelihood [3]

**Consequence**

| Level | Descriptor | Description |
|---|---|---|
| 1 | Insignificant | No injuries, low financial loss. |
| 2 | Minor | First aid treatment required, on-site release immediately contained, medium financial loss. |
| 3 | Moderate | Medical treatment required, on-site release contained with outside assistance, high financial loss. |
| 4 | Major | Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss. |
| 5 | Catastrophic | Death, toxic release off-site with detrimental effect, huge financial loss |

Note: Measures used should reflect the needs and nature of the organisation and activity.

**Likelihood**

| Level | Descriptor | Description |
|---|---|---|
| A | Certain | Is expected to occur in most circumstances. |
| B | Likely | Will probably occur at some time. |
| C | Possible | Might occur at some time. |
| D | Unlikely | Could occur at some time. |
| E | Rare | May occur only in exceptional circumstances. |

Note: These tables need to be tailored to meet the needs of an individual organisation.

[3] Safety Management Systems – An Aviation Business Guide, Civil Aviation Safety Authority, Canberra, 2007

**Table 2: Matrix of consequence and likelihood**

**Australian Standards and New Zealand Standards (1999).**
AS/NZS 4360 Risk Management. Australia: Standards Australia.

| | Consequences | | | | |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Catastrophic |
| Likelihood | 1 | 2 | 3 | 4 | 5 |
| A (certain) | H | H | E | E | E |
| B (likely) | M | H | H | E | E |
| C (moderate) | L | M | H | E | E |
| D (unlikely) | L | L | M | H | E |
| E (rare) | L | L | M | H | H |

**Key**

E: Extreme risk, immediate action required.

H: High risk; senior management responsibility must be specified.

M: Moderate risk; management responsibility must be specified.

L: Low risk; manage by routine procedures.

**Table 3: Transport Canada Civil Avation Risk Matrix[4]**

This risk matrix is designed to help determine the level of risk for a particular hazard by providing objective criteria relating to probability and severity.

| |
|---|
| Low |
| Medium |
| High |

| Probability | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 5 | 10 | 15 | 20 | 25 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| | 1 | 2 | 3 | 4 | 5 |
| | | | Severity | | |

| Values | Risk Levels | Action |
|---|---|---|
| 1–5 | Low | Proceed after considering all elements of risk. |
| 6–12 | Medium | Continue after taking appropriate mitigating action. |
| 13–25 | High | STOP: do not proceed until sufficient control measures have been implemented to reduce risk to an acceptable level. |

| Severity (S) | |
|---|---|
| Level 1 | • No damage or injury or adverse consequences. |
| Level 2 | • Personnel—first aid injury; no disability or lost time<br>• Public—minor impact<br>• Environment—contained release<br>• Equipment—minor damage; potential organizational slowdown or potential downtime |
| Level 3 | • Personnel—lost time injury; no disability<br>• Public—greater than minor impact, loss of confidence; some injury potential<br>• Environment—small uncontained release<br>• Equipment—minor damage; leads to organizational slowdown or minor downtime |
| Level 4 | • Personnel—disability or severe injury<br>• Public—exposed to a hazard that could or will produce injuries<br>• Environment—moderate uncontained release<br>• Equipment—major damage; results in major slowdown or downtime |
| Level 5 | • Personnel—fatal, life-threatening injury<br>• Public—exposed to life-threatening hazard<br>• Environment—large uncontained release<br>• Equipment—loss of critical equipment, or shutdown of organization |
| **Probability (P)** | |
| Level 1 | • Mishap almost impossible. |
| Level 2 | • Postulated event (may be possible, but not known to have occurred). |
| Level 3 | • Has occurred rarely (known to have happened, but a statistically credible frequency cannot be determined). |
| Level 4 | • May/has occur(ed) infrequently. |
| Level 5 | • May/has occur(ed) frequently. |

[4] Transport Canada Advisory Circular, *Safety Management Systems Development Guide for Small Operators/ Organizations*, Ottawa, 2008