SCAA

DOC N°: SCAP 007-002

Sudan Safety Management Manual

Second Edition, February 2019

Issued and Published under the Authority of the Director General

SUDAN CIVIL AVIATION AUTHORITY
THE REPUBLIC OF SUDAN

(February 2019)

SCAA

DOC N^{o}: SCAP 007-002

Document Distribution No.:
Sudan Safety Management Manual
Second Edition, February 2019

Issued and published under the authority of the Director General

SUDAN CIVIL AVIATION AUTHORITY
THE REPUBLIC OF SUDAN

(February 2019)

PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION – AUTHORITY TO PUBLISH

The Sudan Civil Aviation Safety Publication **"Sudan Safety Management Manual"** contains the requirements for services providers to establish and maintain safety management system acceptable to the Authority and commensurate with the size of the service provider and the complexity of its aviation products or services.

This document provides material of factual information and references to Sudan Civil Aviation Regulations (SUCARs) Part 19, on the framework of the Safety management System.

a) In accordance with section 4.1 of SUCAR 19, the SMS of the following services providers shall be made acceptable to the Authority: approved training organizations in accordance with Annex 1 that are exposed to safety risks related to aircraft operations during the provision of their services;
b) operators of aeroplanes or helicopters authorized to conduct international commercial air transport, in accordance with SUCAR Part 6, subpart I or subpart III, Section II, respectively;
c) approved maintenance organizations providing services to operators of aeroplanes or helicopters engaged in international commercial air transport, in accordance with SUCAR Part 6, subpart I or subpart III, Section II, respectively;;
d) organizations responsible for the type design or manufacture of aircraft, engines or propellers in accordance with SUCAR PART 8;
e) air traffic services (ATS) providers in accordance with SUCAR PART 11;
f) operators of certified aerodromes in accordance with SUCAR PART 14, subpart I; and
g) approved ground handling service providers in accordance to SUCAR Part 6, Subpart I Chapter 15

To facilitate the development and implementation of the services providers' safety management systems, this Sudan Civil Aviation Safety Publication provides details on the framework elements of a safety management system.
The material is grouped separately for convenience. However, it forms an integral part of the Standards applicable in Sudan for safety management system, as established in SUCAR Part 19, second edition.
This document is approved and issued under the authority of the Director General, Sudan Civil Aviation Authority.

Capt. Mostafa Said Ahmed Eldwahy
DirectorGeneral, SCAA
February 2019

PAGE INTENTIONALLY LEFT BLANK

RECORDS OF AMENDMENTS

The space below is provided to keep a record of amendments.

Amendment No.	Date of entry	Entered by	signature

PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

PAGE INTENTIONALLY LEFT BLANK

Abbreviations

AAICD	Aircraft Accident and Incident Investigation Central Directorate
ADREP	Accident/incident data reporting
AIR	Airworthiness Directorate
ALoSP	Acceptable Level of Safety Performance
ANRD	Air Navigation Services Regulatory Directorate
ASD	Aviation Safety Department
ATC	Air traffic Control
ATM	Air Traffic Management
DASS	Directorate of Aerodrome Safety & Standards
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
IRM	Integrated Risk Management
MOR	Mandatory Occurrence Reporting
NSDRC	National safety Data review Committee
NSP	National Safety Programme
OPS	Flight Operations Directorate
PEL	Personnel Licensing Department
QMS	Quality Management System
SA	Safety Assurance
SCAA	Sudan Civil Aviation Authority
SCASPs	Sudan Civil Aviation Safety Publications
SMS	Safety Management System
SPI	Safety Performance Indicator
SPS	Safety Policy & Standards Directorate
SPT	Safety Performance Target
SRM	Safety Risk Management
SSDCPS	Sudan safety data collection and processing system
SSMM	Sudan Safety management manual
SSP	State safety programme
SUCARs	Sudan Civil Aviation Regulations
VFR	Visual Flight Rules

PAGE INTENTIONALLY LEFT BLANK

List of Effective Pages

Chapter	Page	Date
Foreword	I	31 January 2019
Abbreviations	Iii	31 January 2019
Record of Amendments	Iv	31 January 2019
List of Effective Pages	V	31 January 2019
Table of Contents	Vi	31 January 2019
CHAPTER 1 - Introduction	1-1 to 1-7	31 January 2019
CHAPTER 2 – SMS framework	2-1	31 January 2019
CHAPTER 3 – Safety policy and objectives	3-1 to 3-9	31 January 2019
CHAPTER 4– Safety risk management	4-1 to 4-17	31 January 2019
CHAPTER 5 – Safety assurance	5-1 to 5-12	31 January 2019
CHAPTER 6 – Safety promotion	6-1 to 6-4	31 January 2019
CHAPTER 7 – SMS implementation	7-1 to 7-5	31 January 2019
CHAPTER 8 – Safety data collection, processing and exchange	8-1 to 8-11	31 January 2019

PAGE INTENTIONALLY LEFT BLANK

Chapter 1 – Introduction

1.1. Definitions

The definitions used in this publication are similar to those found in the Sudan National Safety Program, relevant Sudan Civil Aviation Regulations and guidance material (such as SUCAR 19, Operational Policy on the aviation safety reporting system, and associated documentation) or are the definitions intended for this document and the SCAA safety reporting system as given below:

Acceptable level of safety performance (ALoSP). The level of safety performance agreed by State authorities to be achieved for the civil aviation system in a State, as defined in its State safety programme, expressed in terms of safety performance targets and safety performance indicators.

Accountable executive. A single, identifiable person having responsibility for the effective and efficient performance of the service provider's SMS.

Authority. *Sudan Civil Avaition Authority*

Change management. A formal process to manage changes within an organization in a systematic manner, so that changes which may impact identified hazards and risk mitigation strategies are accounted for, before the implementation of such changes.

Defences. Specific mitigating actions, preventive controls or recovery measures put in place to prevent the realization of a hazard or its escalation into an undesirable consequence.

Errors. An action or inaction by an operational person that leads to deviations from organizational, or the operational person's, intentions or expectations.

Hazard. A condition or an object with the potential to cause or contribute to an aircraft incident or accident.

Risk mitigation. The process of incorporating defences, preventive controls or recovery measures to lower the severity and/or likelihood of a hazard's projected consequence.

Safety. The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level.

Safety data. A defined set of facts or set of safety values collected from various

aviation-related sources, which is used to maintain or improve safety.
It is generally collected from proactive or reactive safety-related activities, including but no limited to:

a) accident or incident investigations;
b) safety reporting;
c) continuing airworthiness reporting;
d) operational performance monitoring;
e) inspections, audits, surveys; or
f) safety studies and reviews.

Safety information. Safety data processed, organized or analysed in a given context so as to make it useful for safety management purposes.

Safety management system (SMS). A systematic approach to managing safety, including the necessary organizational structures, accountability, responsibilities, policies and procedures.

Safety objective. A brief, high-level statement of safety achievement or desired outcome to be accomplished by the National safety programme or service provider's safety management system. They are developed from the organization's top safety risks and shall be taken into consideration during subsequent development of safety performance indicators and targets.

Safety oversight. A function performed by a State to ensure that individuals and organizations performing an aviation activity comply with safety-related national laws and regulations.

Safety performance. A State's or service provider´s safety achievement as defined by its safety performance targets and safety performance indicators.

Safety performance indicator. A data-based parameter used for monitoring and assessing safety performance.

Safety performance target. The State or service provider's planned or intended target for a safety performance indicator over a given period that aligns with the safety objectives.

Safety risk. The predicted probability and severity of the consequences or outcomes of a hazard.

System. An organized, purposeful structure that consists of interrelated and

interdependent elements and components, and related policies, procedures and practices created to carry out a specific activity or solve a problem.

Trigger. An established level or criteria value for a particular safety performance indicator that serves to initiate an action required, (e.g., an evaluation, adjustment or remedial action).

1.2. Requirements for safety management system

The requirements for safety management system are contained in chapter 4 of SUCAR 19. It identifies the service providers which are required to establish an SMS. Appendix B to SUCAR 19 further specifies the components and elements of an SMS.

1.3. Objectives of safety management system

Safety management seeks to proactively mitigate safety risks before they result in aviation accidents and incidents. Through the implementation of safety management system, a service provider can manage its safety activities in a more disciplined, integrative and focused manner. Possessing a clear understanding of its role and contribution to safe operations enables a service provider to prioritize actions to address safety risks and more effectively manage its resources for the optimal benefit of aviation safety.

The purpose of an SMS is to provide service providers with a systematic approach to managing safety. It is designed to continuously improve safety performance through: the identification of hazards, the collection and analysis of safety data and safety information, and the continuous assessment of safety risks. An effective SMS demonstrates to the Authority the service provider's ability to manage safety risks and provides for effective management of safety at the State level.

1.4. Applicability for State-owned or military service providers

In some instances, the service provider function may be provided by a Sudan civil service or military. Also, civilian service providers may provide contracted services to the military, and some military organizations may provide civilian service.

Regardless of the arrangement, the service provider for the civilian service in the State is required to address all the applicable SUCARs requirements, including the SUCAR 19 SMS requirements without regard to the specific nature of such organization. The State's or service provider's system description shall have regard for the functions of these organizations and their relationship to each other. The accountable

executive of the service provider, whether civil or military, is responsible for explaining the arrangements and how safety risks are managed. But simply, service providers should manage safety regardless of the organizational arrangements.

Where the Authority operates as a service provider there shall be a clear separation between its functions as the service provider and that of regulatory authority. This is accomplished by having clearly defined roles and responsibilities for regulatory authority and service provider personnel to avoid any conflicts of interest.

1.5. Occupational safety, health and environment versus aviation safety

Occupational safety, health and environment (OSHE) (also referred as occupational health and safety (OHS) or workplace health and safety (WHS)) is a field concerned with the safety, health, and welfare of people at work. The primary difference between aviation safety management and OSHE systems is the intent. Employers have a legal duty to take reasonable care of the health and safety of their employees. The intention of OSHE programmes is to meet the legal and ethical obligations of employers by fostering a safe and healthy work environment.

These issues are not addressed by the Sudan Civil Aviation Authority . As such, SUCA 19, Chapter 2, *Applicability*, intentionally focuses on "safety management functions related to, or in direct support of, the safe operation of aircraft".

1.6. Implementing safety management

Establishing a solid foundation is essential to achieving effective safety management implementation. The following aspects shall be addressed as the first steps in implementing SMS requirements:

a) *Senior management commitment*: It is essential that senior management of a service provider is committed to effective safety management implementation.

b) *Compliance with prescriptive requirements*: The Service provider shall ensure that it has processes in place to ensure continued compliance with the established prescriptive requirements.

1.7. System description

The system description is a summary of the service provider's processes, activities and interfaces that need to be assessed for hazard identification and safety risk assessment that is covered by its safety system. It describes the aviation system, within which the service provider functions, and the various entities involved. It includes interfaces within the organization, as well as interfaces with external organizations

that contribute to the safe delivery of services. The system description provides a starting point to implement the SMS.

1.8. Interfaces

When a service provider is considering implementing safety management it is important to consider the safety risks induced by interfacing entities. Interfaces can be internal (e.g. between operations and maintenance, or finance, human resources or legal departments), or they can be external (e.g. other service providers or contracted services). A service provider has greater control over any related safety risks when interfaces are identified and managed. Interfaces are defined as part of the system description.

1.8.1. Interface safety impact assessment

Once a service provider has identified its interfaces, the safety risk posed by each interface is assessed using the organization's existing safety risk assessment processes. Based on the safety risks identified, the service provider may consider working with other organizations to determine an appropriate safety risk control strategy. Organizations working collaboratively may be able to identify more interface hazards; assessing any related safety risks and determining mutually appropriate controls. Collaboration is highly desirable because the safety risk perception may vary between organizations.

It is also important to recognize that each organization involved is responsible for identifying and managing any identified hazards that affect its organization. The criticality of the interface may differ for each organization. Each organization might reasonably apply different safety risk classifications and have different safety risk priorities (in terms of safety performance, resources, time).

1.8.2. Monitoring and management of interfaces

Each service provider is responsible for ongoing monitoring and management of its interfaces to ensure the safe provision of services. This is achieved through establishment of formal agreements between interfacing organizations with clearly defined monitoring and management responsibilities. Documenting and sharing all interface safety issues, safety reports and lessons learned, as well as safety risks between interfacing organizations will ensure clear understanding. Sharing enables transfer of knowledge and working practices that could improve the safety effectiveness of each organization.

1.8.3. Implementation planning

Pursuant to 4.1.2 of SUCAR 19, a service provider is required to perform a gap analysis and develop an implementation plan before embarking on the implementation of SMS. The gap analysis allows the service

provider to identify the gap between the current organizational structures and processes, and those required for effective SMS operation.

The SMS implementation plan is, as the name implies, a plan for SMS implementation. It provides a clear description of the resources, tasks and processes required, and an indicative timing and sequencing of key tasks and responsibilities.

1.8.4. Maturity assessment

Soon after the key components and elements of the SMS are implemented, periodic assessments shall be conducted to monitor how effectively it is working. As the system matures, the service provider shall seek assurance that it is operating as intended and is effective at achieving its stated safety objectives and targets. Safety management takes time to mature and the aim shall be to maintain or continuously improve the safety performance of the organization.

1.8.5. Size and complexity considerations

Each service provider is different. SMSs are designed to be tailored to meet the specific needs of each service provider. All components and all elements of the SMS are interconnected and interdependent, and necessary to function effectively. It is important that SMS requirements are not implemented only in a prescriptive manner. The traditional prescriptive requirements are to be complemented with a performance-based approach.

The system is designed to deliver the desired outcomes for each organization without undue burden. SMS, well implemented, is intended to complement and enhance the organization's existing systems and processes. Effective safety management will be achieved through thoughtful planning and implementation, ensuring each requirement is addressed in ways that fit the organization's culture and operating environment respectively.

1.8.6. Integrating the basic elements

It is important to note that all systems are composed of three basic elements: people; processes; and technology. Safety management is no exception. When establishing or maintaining the different processes, activities and functions, all service providers must ensure they have considered the intention of each requirement and, most importantly, how they will work together to enable the organization to meet its safety objectives.

1.9. Integrated Risk Management

The aviation system as a whole comprises many and different functional systems such as finance, environment, safety and security. The latter two are the primary operational domains of the greater aviation system. As concepts they share important features as they are all concerned with the risk of events with consequence of various magnitudes.

Nevertheless, they differ in the important element of intent. Security is concerned with malicious, intentional acts to disrupt the performance of a system. Safety focuses on the negative impact to the concerned systems' performance caused by unintended consequences of a combination of factors.

In the operational context, all of the functional systems produce some sort of risk that needs to be appropriately managed to lessen any adverse consequence. Traditionally, each system has developed sector specific risk management frameworks and practices designed to address the distinct characteristics of each system. Most of those risk management practices include comprehensive analysis on intra-system consequences, often referred to as the management of unintended consequences. Another aspect is inter-system consequences resulting from system specific risk management processes. This relates to the fact that an effective risk management strategy of one specific sector can have an adverse impact on another operational sector of aviation. In aviation, the most often emphasized inter-system dependence is the safety/security dilemma. Effective security measures may have negative impacts on safety, and vice versa. Safety and security domains may differ in the element of underlying intent, but they converge in their common goal to protect people and assets (e.g. addressing cyber threats and risks requires coordination across the aviation safety and security domains). In some cases the management of the inherent risk of one may affect the
other domain in unforeseen ways, such as in the following examples:

a) reinforced cockpit doors necessitated due to security risks may have safety implications on the operation of an aircraft;
b) restrictions on the carriage of personal electronic devices in the cabin may displace the security risk from the cabin to the cargo hold, leading to heightened safety risk; and
c) change of routes to avoid flying over conflict zones may result in congested air corridors that pose a safety issue.

Successful risk management in aviation requires the analytical assessment of the whole system at the highest level of the appropriate entity. The assessment and integration of functional system needs and interdependence are referred to as integrated risk management (IRM). IRM focuses on the overall risk reduction of the organization. This is achieved through the quantitative and qualitative analysis of both the inherent risks, and the effectiveness and impact of sector-specific risk management processes. IRM has a system-wide responsibility to coordinate, harmonize and optimize risk management processes with the single goal of risk reduction. IRM cannot replace the operating specific

risk managements of the functional systems, and does not intend to delegate additional duties and responsibilities to them. IRM is a distinct high-level concept to leverage the expert advice of sector specific risk management and provide holistic feedback to achieve the highest level of system performance at a socially acceptable level.

Chapter 2 – SMS framework

2.1. General

SUCAR 19 specifies the framework for the implementation and maintenance of an SMS. Regardless of the service provider's size and complexity, all elements of the SMS framework apply. The implementation shall be tailored to the service provider and its activities.

2.2. SMS Components and elements

The Sudan SMS framework is made up of the following four components and twelve elements:

Component	Element
Safety policy and objectives	Management commitment
	Safety accountability and responsibilities
	Appointment of key safety personnel
	Coordination of emergency response planning
	SMS documentation
Safety risk management	Hazard identification
	Safety risk assessment and mitigation
Safety assurance	. Safety performance monitoring and measurement
	. The management of change
	. Continuous improvement of the SMS
Safety promotion	. Training and education
	. Safety Communication

Table 2-1 SMS Components and elements

Chapter 3 – Safety Policy and Objectives

3.1. General

The first component of the SMS framework focuses on creating an environment where safety management can be effective. It is founded on a safety policy and objectives that set out senior management's commitment to safety, its goals and the supporting organizational structure.

Management commitment and safety leadership are key to the implementation of an effective SMS and are asserted through the safety policy and the establishment of safety objectives.

Management commitment to safety is demonstrated through management decision-making and allocation of resources; these decisions and actions shall always be consistent with the safety policy and objectives to cultivate a positive safety culture.

The safety policy shall be developed and endorsed by senior management, and is to be signed by the accountable executive. Key safety personnel, and where appropriate, staff representative bodies (employee forums, trade unions) shall be consulted in the development of the safety policy and safety objectives to promote a sense of shared responsibility.

3.2. Management commitment

3.2.1. Safety Policy

The safety policy shall be visibly endorsed by senior management and the accountable executive. "Visible endorsement" refers to making management's active support of the safety policy visible to the rest of the organization. This can be done via any means of communication and through the alignment of activities to the safety policy.

It is the responsibility of management to communicate the safety policy throughout the organization to ensure all personnel understand and work in accordance with the safety policy.

To reflect the organization's commitment to safety, the safety policy shall include a commitment to:

a) continuously improve the level of safety performance;
b) promote and maintain a positive safety culture within the organization;
c) comply with all applicable regulatory requirements;
d) provide the necessary resources to deliver a safe product or service;

e) ensure safety is a primary responsibility of all managers; and
f) ensure it is understood, implemented and maintained at all levels.

The safety policy shall also make reference to the safety reporting system to encourage the reporting of safety issues and inform personnel of the disciplinary policy applied in the case of safety events or safety issues that are reported.

The disciplinary policy is used to determine whether an error or rule breaking has occurred so that the organization can establish whether any disciplinary action should be taken. To ensure the fair treatment of persons involved, it is essential that those responsible for making that determination have the necessary technical expertise so that the context of the event may be fully considered.

A policy on the protection of safety data and safety information, as well as reporters, can have a positive effect on the reporting culture. The service provider shall allow for the de-identification and aggregation of reports to allow meaningful safety analyses to be conducted without having to implicate personnel or specific service providers. Because major occurrences may invoke processes and procedures outside of the service provider's SMS, the Authority may not permit the early de-identification of reports in all circumstances. Nonetheless, a policy allowing for the appropriate de-identification of reports can improve the quality of data collected.

3.2.2. Safety Objectives

Taking into consideration its safety policy, the service provider shall also establish safety objectives to define what it aims to achieve in respect of safety outcomes. Safety objectives must be short, high-level statements of the organization's safety priorities and shall address its most significant safety risks.

Safety objectives define what the organization intends to achieve in terms of safety. Safety performance indicators (SPIs) and safety performance targets (SPTs) are needed to monitor the achievement of these safety objectives.

The safety policy and safety objectives shall be periodically reviewed to ensure they remain current (a change in the accountable executive would require its review for instance).

3.3. Safety accountabilities and responsibilities

3.3.1. Accountable Executive

The accountable executive, typically the chief executive officer, is the person who has ultimate authority over the safe operation of the organization. The accountable executive establishes and promotes the safety policy and safety objectives that instill safety as a core organizational value. He/she must:

a) have the authority to make decisions on behalf of the organization,
b) have control of resources, both financial and human,
c) be responsible for ensuring appropriate actions are taken to address safety issues and safety risks, and
d) be responsible for responding to accidents and incidents.

The service provider is required to identify the accountable executive, placing the responsibility for the overall safety performance at a level in the organization with the authority to take action to ensure the SMS is effective.

3.3.2. One legal entity with multiple certificates, authorizations or approvals

In the case where an SMS applies to several different certificates, authorizations or approvals that are all part of the same legal entity, there should be a single accountable executive. Where this is not possible, individual accountable executives may be identified for each organizational certificate, authorization or approval and clear lines of accountability defined; it is also important to identify how their safety accountabilities will be coordinated.

3.3.3. Involvement of the accountable executive

The accountable executive shall lead regular executive safety meetings to:

a) review safety objectives;
b) monitor safety performance and the achievement of safety targets;
c) make timely safety decisions;
d) allocate appropriate resources;
e) hold managers accountable for safety responsibilities, performance and implementation timelines; and
f) be seen by all personnel as an executive who is interested in, and in charge of, safety.

The outcomes of such executive meetings shall be documented and be available, their implementation thereafter monitored, and made available for inspection by the Authority during surveillance inspections.

3.3.4. Delegation

The accountable executive is not usually involved in the day-to-day activities of the organization or the problems faced in the workplace and shall ensure there is an appropriate organizational structure to manage and operate the SMS. Safety management responsibility is often delegated to the senior management team and other key safety personnel.

3.3.5. Limits of delegation

Although responsibility for the day-to-day operation of the SMS can be delegated, the accountable executive cannot delegate accountability for the system nor can decisions regarding safety risks be delegated. For example, the following safety accountabilities cannot be delegated:

a) ensuring safety policies are appropriate and communicated;
b) ensuring necessary allocation of resources (financing, personnel, training, acquisition); and
c) setting of the acceptable safety risk limits and resourcing of necessary controls.

3.3.6. Accountabilities of the accountable executive

The accountable executive to have the following safety accountabilities:

a) provide enough financial and human resources for the proper implementation of an effective SMS;
b) promote a positive safety culture;
c) establish and promote the safety policy;
d) establish the organization's safety objectives;
e) ensure the SMS is properly implemented and performing to requirements; and
f) see to the continuous improvement of the SMS.

3.3.7. Authorities of the accountable executive

The accountable executive's authorities include, but are not limited to, having final authority:

a) for the resolution of all safety issues; and
b) over operations under the certificate, authorization or approval of the organization, including the authority to stop the operation or activity.

The authority to make decisions regarding safety risk tolerability shall be defined. This includes who can make decisions on the acceptability of risks as well as the authority to agree that a change can be implemented. The authority may be assigned to an individual, a management position or a committee.

Authority to make safety risk tolerability decisions should be commensurate with the manager's general decision-making and

resource allocation authority. A lower level manager (or management group) may be authorized to make tolerability decisions up to a certain level. Risk levels that exceed the manager's authority must be escalated for consideration to a higher management level with greater authority.

3.3.8. Accountabilities and responsibilities of senior management and personnel

Accountabilities and responsibilities of all personnel, management and staff, involved in safety-related duties supporting the delivery of safe products and operations shall be clearly defined. The safety responsibilities shall focus on the staff member's contribution to the safety performance of the organization (the organizational safety outcomes). The management of safety is a core function; as such every senior manager has a degree of involvement in the operation of the SMS.

All defined accountabilities, responsibilities and authorities shall be stated in the service provider's SMS documentation and shall be communicated throughout the organization. The safety accountabilities and responsibilities of each senior manager are integral components of their job descriptions. This shall also capture the different safety management functions between line managers and the safety manager.

Lines of safety accountability throughout the organization and how they are defined will depend on the type and complexity of the organization, and their preferred communication methods. Typically, the safety accountabilities
and responsibilities will be reflected in organizational charts, documents defining departmental responsibilities, and personnel job or role descriptions.

The service provider shall aim to avoid conflicts of interest between staff members' safety responsibilities and their other organizational responsibilities. They shall allocate their SMS accountabilities and responsibilities, in a way that minimizes any overlaps and/or gaps.

3.3.9. Accountability and responsibilities and in respect to external organizations

A service provider is responsible for the safety performance of external organizations where there is an SMS interface. The service provider may be held accountable for the safety performance of products or services provided by external organizations supporting its activities even if the external organizations are not required to have an SMS. It is essential for the service provider's SMS to interface with the safety systems of any external organizations that contribute to the safe delivery of their product or services.

3.4. Appointment of key safety personnel

3.4.1. Safety Manager

The service provider will appoint a safety manager to be responsible to the accountable executive for the performance of the SMS and for the delivery of safety services to the other departments in the organization.

Depending on the size, nature and complexity of the organization, the safety manager role may be an exclusive function or it may be combined with other duties. Moreover, the size and complexity of operations may dictate to allocate the role to a group of persons. The organization must ensure that the option chosen does not result in any conflicts of interest. Where possible, the safety manager should not be directly involved in the product or service delivery but should have a working knowledge of these. The appointment should also consider potential conflicts of interest with other tasks and functions. Such conflicts of interest could include:

a) competition for funding (e.g. financial manager being the safety manager);
b) conflicting priorities for resources; and
c) where the safety manager has an operational role and the ability to assess the SMS effectiveness of the operational activities the safety manager is involved in.

In cases where the function is allocated to a group of persons, (e.g. when service providers extend their SMS across multiple activities) one of the persons shall be designated as “lead” safety manager, to maintain a direct and unequivocal reporting line to the accountable executive.

3.4.1.1. Functions of the Safety Manager

The safety manager advises the accountable executive and line managers on safety management matters, and is responsible for coordinating and communicating safety issues within the organization as well as with external members of the aviation community. Functions of the safety manager include, but are not limited to:

a) manage the SMS implementation plan on behalf of the accountable executive (upon initial implementation);
b) perform/facilitate hazard identification and safety risk analysis;
c) monitor corrective actions and evaluate their results;
d) provide periodic reports on the organization’s safety performance;
e) maintain SMS documentation and records;
f) plan and facilitate staff safety training;
g) provide independent advice on safety matters;
h) monitor safety concerns in the aviation industry and their perceived impact on the organization’s operations aimed at product and service delivery; and

i) coordinate and communicate (on behalf of the accountable executive) with the Authority and other Sudan authorities as necessary on issues relating to safety.

3.4.1.2. Qualification requirements for the Safety Manager

The competencies for a safety manager shall include, but not be limited to, the following:

a) a minimum of 3 years safety/quality management experience;
b) a minimum of 5 years operational experience related to the product or service provided by the organization;
c) technical background to understand the systems that support operations or the product/service provided;
d) interpersonal skills;
e) analytical and problem-solving skills;
f) project management skills;
g) oral and written communications skills; and
h) an understanding of human factors.

3.4.1.3. Acceptability of the safety manager by the Authority

Prior to his/her appointment, the candidate for the position of safety manager shall be submitted to the SPS for acceptance following the process sets out by the SPS.

3.4.1.4. Safety management's support staff

Depending on the size, nature and complexity of the organization, additional staff may support the safety manager. The safety manager and supporting staff are responsible for ensuring the prompt collection and analysis of safety data and appropriate distribution within the organization of related safety information such that safety risk decisions and controls, as necessary, can be made.

3.4.2. Safety Committees

Service providers shall establish safety committees, to include:

1) Safety Review Board (SRB), and
2) Safety Action Groups (SAG).

3.4.2.1. Safety Review Board

The safety review board (SRB), includes the accountable executive and senior managers with the safety manager participating in an advisory capacity. The SRB is strategic and deals with high-level issues related to safety policies, resource allocation and organizational performance. The SRB monitors the:

1) effectiveness of the SMS;
2) timely response in implementing necessary safety risk control actions;

3) safety performance against the organization's safety policy and objectives;
4) overall effectiveness of safety risk mitigation strategies;
5) effectiveness of the organization's safety management processes which support:
   a) the declared organizational priority of safety management; and
   b) promotion of safety across the organization.

Once a strategic direction has been developed by the highest-level safety committee, implementation of safety strategies shall be coordinated throughout the organization by the safety action groups (SAGs) that are more operationally focused.

3.4.2.2. Safety Action Groups

Service providers shall establish one or more safety action groups (SAG) as tactical entities that deal with specific implementation issues in accordance with the strategies developed by the SRB. The SAGs:

a) monitor operational safety performance within their functional areas of the organization and ensure that appropriate safety risk management (SRM) activities are carried out;
b) review available safety data and identify the implementation of appropriate safety risk control strategies and ensure employee feedback is provided;
c) assess the safety impact related to the introduction of operational changes or new technologies;
d) coordinate the implementation of any actions related to safety risk controls and ensure that actions are taken promptly; and
e) review the effectiveness of specific safety risk controls.

3.5. Coordination of emergency response planning

Coordination of emergency response planning (ERP) applies only to those service providers required to establish and maintain an ERP. SUCAR 19 does not require the creation or development of an ERP; emergency response planning is applicable only to specific service providers as established in the relevant SUCAR This coordination should be exercised as part of the periodic testing of the ERP.

An emergency response plan (ERP) is an integral component of a service provider's SRM process to address aviation-related emergencies, crises or events. Where there is a possibility of a service provider's aviation operations or activities being compromised by emergencies such as a public health emergency/pandemic, these scenarios must also be addressed in its ERP as appropriate.

The ERP shall address foreseeable emergencies as identified through the SMS and include mitigating actions, processes and controls to effectively manage aviation-related emergencies.

The ERP shall be easily accessible to the appropriate key personnel as well as to the coordinating external organizations.

3.6. SMS Documentation

The service shall establish and maintain SMS documentation that includes:

a) a top-level “SMS manual”, and
b) compilation and maintenance of operational records substantiating the existence and ongoing operation of the SMS

The SMS manual describes the service provider’s SMS policies, processes and procedures to facilitate the organization’s internal administration, communication and maintenance of the SMS. It is intended to help personnel to understand how the organization’s SMS functions, and how the safety policy and objectives will be met. It shall also help clarify the relationship between the various policies, processes, procedures and practices, and define how these links to the service provider’s safety policy and objectives.

The SMS manual also serves as a primary safety communication tool between the service provider and key safety stakeholders (e.g. SCAA for the purpose of regulatory acceptance, assessment and subsequent monitoring of the SMS). The SMS manual may be a stand-alone document, or it may be integrated with other organizational documents (or documentation) maintained by the service provider. Where details of the organization’s SMS processes are already addressed in existing documents, appropriate cross-referencing to such documents is enough. This SMS document must be kept up to date. SCAA agreement is required before significant amendments are made to the SMS manual, as it is a controlled manual.

The SMS manual shall include a detailed description of the service provider’s policies, processes and procedures including:

1) safety policy and safety objectives;
2) reference to any applicable regulatory SMS requirements;
3) system description that provides the boundaries of the SMS;
4) safety accountabilities and key safety personnel;
5) voluntary and mandatory safety reporting system processes and procedures;

6) hazard identification and safety risk assessment processes and procedures;
7) safety investigation procedures;
8) procedures for establishing and monitoring safety performance indicators;
9) SMS training processes and procedures and communication;
10) safety communication processes and procedures;
11) internal audit procedures;
12) management of change procedures;
13) SMS documentation management procedures; and
14) where applicable, coordination of emergency response planning.

SMS documentation also includes the compilation and maintenance of operational records substantiating the existence and ongoing operation of the SMS. Operational records are the outputs of the SMS processes and procedures such as the SRM and safety assurance activities. SMS operational records shall also be stored and kept in accordance with existing retention periods. SMS operational records include:

a) hazards register and hazard/safety reports;
b) SPIs and related charts;
c) record of completed safety risk assessments;
d) SMS internal review or audit records;
e) internal audit records;
f) records of SMS/safety training records;
g) SMS/safety committee meeting minutes;
h) SMS implementation plan (during the initial implementation); and
i) gap analysis to support implementation plan.

The service provider shall ensure that the SMS documentation is understood by personnel throughout the organization.

Chapter 4 – Safety Risk Management

4.1. General

Service providers shall establish and implement method, procedures and processes for managing their safety risks. This process is known as safety risk Management (SRM), which includes hazard identification, safety risk assessment and safety risk mitigation.

The SRM process systematically identifies hazards that exist within the context of the delivery of its products or services. Hazards may be the result of systems that are deficient in their design, technical function, human interface or interactions with other processes and systems. They may also result from a failure of existing processes or systems to adapt to changes in the service provider's operating environment. Careful analysis of these factors can often identify potential hazards at any point in the operation or activity life cycle.

Understanding the system and its operating environment is essential for the achievement of high safety performance. Having a detailed system description that defines the system and its interfaces will help. Hazards may be identified throughout the operational life cycle from internal and external sources. Safety risk assessments and safety risk mitigations will need to be continuously reviewed to ensure they remain effective. Figure 4-1 provides an overview of the hazard identification and safety risk management process for a service provider.

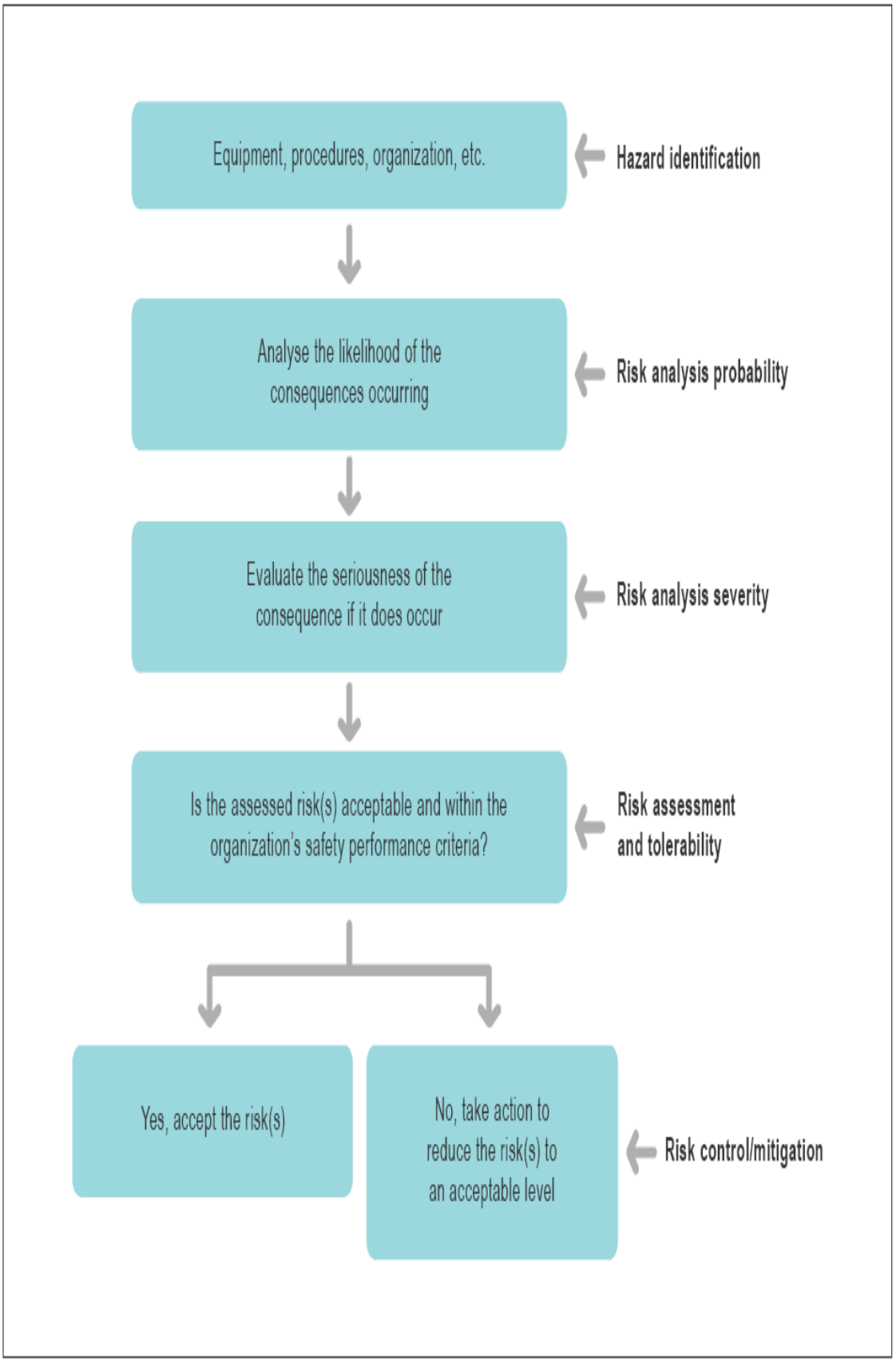

Figure 4 – 1: Hazard identification and risk management process

4.2. Hazard identification

Hazard identification is the first step in the SRM process. The service provider shall develop and maintain a formal process to identify hazards that could impact aviation safety in all areas of operation and activities. This includes equipment, facilities and systems. Any aviation safety-related hazard identified and controlled is beneficial for the safety of the operation. It is important to also consider hazards that may exist as a result of the SMS interfaces with external organizations.

The process for identifying hazards shall be documented in the SMS documentation.

4.2.1. Objectives of hazard identification

The goal is to proactively identify hazards before they lead to accidents, incidents or other safety-related occurrences.

4.2.2. Mechanism for hazard identification

An important mechanism for proactive hazard identification is a voluntary safety reporting system. Information collected through such reporting systems may be supplemented by observations or findings recorded during routine site inspections or organizational audits.

Hazards can also be identified in the review or study of internal and external investigation reports. A consideration of hazards when reviewing accident or incident investigation reports is a good way to enhance the organization's hazard identification system. This is particularly important when the organization's safety culture is not yet mature enough to support effective voluntary safety reporting, or in small organizations with limited events or reports.

Hazard identification may also consider hazards that are generated outside of the organization and hazards that are outside the direct control of the organization, such as extreme weather or volcanic ash. Hazards related to emerging safety risks are also an important way for organizations to prepare for situations that may eventually occur.
The following should be considered when identifying hazards:

a) system description;
b) design factors, including equipment and task design;
c) human performance limitations (e.g. physiological, psychological, physical and cognitive);
d) procedures and operating practices, including documentation and checklists, and their validation under actual operating conditions;
e) communication factors, including media, terminology and language;

f) organizational factors, such as those related to the recruitment, training and retention of personnel, compatibility of production and safety goals, allocation of resources, operating pressures and corporate safety culture;
g) factors related to the operational environment (e.g. weather, ambient noise and vibration, temperature and lighting);
h) regulatory oversight factors, including the applicability and enforceability of regulations, and the certification of equipment, personnel and procedures;
i) performance monitoring systems that can detect practical drift, operational deviations or a deterioration of product reliability;
j) human-machine interface factors; and
k) factors related to the SSP/SMS interfaces with other organizations.

4.2.3. Hazard identification methodologies

The services provider shall document the methodologies established for the identification of hazards. Such methodologies may include:

a) Reactive. This methodology involves analysis of past outcomes or events. Hazards are identified through investigation of safety occurrences. Incidents and accidents are an indication of system deficiencies and therefore can be used to determine which hazard(s) contributed to the event.
b) Proactive. This methodology involves collecting safety data of lower consequence events or process performance and analysing the safety information or frequency of occurrence to determine if a hazard could lead to an accident or incident. The safety information for proactive hazard identification primarily comes from flight data analysis (FDA) programmes, safety reporting systems and the safety assurance function.
c) Predictive: Hazards can also be identified through safety data analysis which identifies adverse trends and makes predictions about emerging hazards, etc.

4.2.4. Sources for hazard identification

The service provider shall document the sources of hazard identification to be used. There are a variety of sources for hazard identification, internal or external to the organization. Some internal sources include:

a) *Normal operations monitoring*: this uses observational techniques to monitor the day-to-day operations and activities such as line operations safety audit (LOSA).
b) *Automated monitoring systems*: this uses automated recording systems to monitor parameters that can be analysed such as flight data monitoring (FDM).

c) *Voluntary and mandatory safety reporting systems*: this provides everyone, including staff from external organizations, with opportunities to report hazards and other safety issues to the organization.
d) *Audits*: these can be used to identify hazards in the task or process being audited. These should also be coordinated with organizational changes to identify hazards related to the implementation of the change.
e) *Feedback from training*: training that is interactive (two way) can facilitate identification of new hazards from participants.
f) *Service provider safety investigations*: hazards identified in internal safety investigation and follow-up reports on accidents/incidents.
g) *Workshops or meetings* : in which subject matter experts conduct detailed analysis scenarios. These sessions benefit from the contributions of a range of experienced operational and technical personnel. Existing safety committee meetings (SRB, SAG, etc.) could be used for such activities.

Examples of external sources for hazard identification include:

a) *Aviation accident reports*; reviewing accident reports; this may be related to accidents in the Sudan, or to a similar aircraft type, region or operational environment.
b) *Authority mandatory and voluntary safety reporting systems*: summaries of the safety reports received from service providers as provided by the Authority.
c) ICAO, trade associations or other international bodies.

4.2.5. Hazards related to SMS interfaces with external organizations

Services providers must also identify hazards related to their safety management interfaces. This should, where possible, be carried out as a joint exercise with the interfacing organizations. The hazard identification must consider the operational environment and the various organizational capabilities (people, processes, technologies) which could contribute to the safe delivery of the service or product's availability, functionality or performance.

4.2.6. Documenting the hazard identification

The hazard identification process considers all possible hazards that may exist within the scope of the service provider's aviation activities including interfaces with other systems, both within and external to the organization.

Identified hazards and their potential consequences should be documented in a hazard register to be maintained by the services provider.

Once hazards are identified, their consequences (i.e. any specific events or outcomes) must be determined.

4.2.7. Investigation of hazards

Hazard identification must be continuous and part of the service provider's ongoing activities. Some conditions may merit more detailed investigation. These may include:

a) instances where the organization experiences an unexplained increase in aviation safety-related events or regulatory non-compliance; or
b) significant changes to the organization or its activities.

4.2.8. Service provider safety investigation

Effective safety management depends on quality investigations to analyse safety occurrences and safety hazards, and report findings and recommendations to improve safety in the operating environment.

There is a clear distinction between accident and incident investigations under SUCAR 13 and service provider safety investigations. Investigation of accidents and serious incidents under SUCAR 13 are the responsibility of the Aircraft Accident and Incidents investigation Directorate, as defined in SUCAR 13. This type of information is essential to disseminate lessons learned from accidents and incidents. Service provider safety investigations are conducted by service providers as part of their SMS to support hazard identification and risk assessment processes. There are many safety occurrences that fall outside of SUCAR 13 that could provide a valuable source of hazard identification or identify weaknesses in risk controls. These problems might be revealed and remedied by a safety investigation led by the service provider.

The primary objective of the service provider safety investigation is to understand what happened, and how to prevent similar situations from occurring in the future by eliminating or mitigating safety deficiencies. This is achieved through careful and methodical examination of the event and by applying the lessons learned to reduce the probability and/or consequence of future recurrences. Service provider safety investigations are an integral part of the service provider's SMS.

Service provider investigations of safety occurrences and hazards are an essential activity of the overall risk management process in aviation. The benefits of conducting a safety investigation include:

a) gaining a better understanding of the events leading up to the occurrence;
b) identifying contributing human, technical and organizational factors;

c) identifying hazards and conducting risk assessments;
d) making recommendations to reduce or eliminate unacceptable risks; and
e) identifying lessons learned that should be shared with the appropriate members of the aviation community.

4.2.8.1. Investigation triggers

A service provider safety investigation is usually triggered by a notification (report) submitted through the safety reporting system. Figure 4-2 outlines the safety investigation decision process and the distinction between when a service provider safety investigation must take place and when an investigation under Annex 13 provisions needs be initiated.
Not all occurrences or hazards can or shall be investigated; the decision to conduct an investigation and its depth depends on the actual or potential consequences of the occurrence or hazard. Occurrences and hazards considered to have a high-risk potential are more likely to be investigated and shall be investigated in greater depth than those with lower risk potential. Service providers shall use a structured decision-making approach with defined trigger points. These will guide the safety investigation decisions: what to investigate and the scope of the investigation. This could include:

a) the severity or potential severity of the outcome
b) regulatory or organizational requirements to carry out an investigation;
c) safety value to be gained;
d) opportunity for safety action to be taken;
e) risks associated with not investigating;
f) contribution to targeted safety programmes;
g) identified trends;
h) training benefit; and
i) resources availability.

4.2.8.2. Assigning an investigator

If an investigation is to commence, the first action will be to appoint an investigator or where the resources are available, an investigation team with the required skills and expertise. The size of the team and the expertise profile of its members depend on the nature and severity of the occurrence being investigated. The investigating team may require the assistance of other specialists. Often, a single person is assigned to carry out an internal investigation, with support from operations and safety office experts.

Service provider safety investigators are ideally organizationally independent from the area associated with the occurrence or identified

hazard. Better results will be obtained if the investigator(s) are knowledgeable (trained) and skilled (experienced) in service provider safety investigations. The investigators would ideally be chosen for the role because of their knowledge, skills and character traits, which should include: integrity, objectivity, logical thinking,
pragmatism, and lateral thinking.

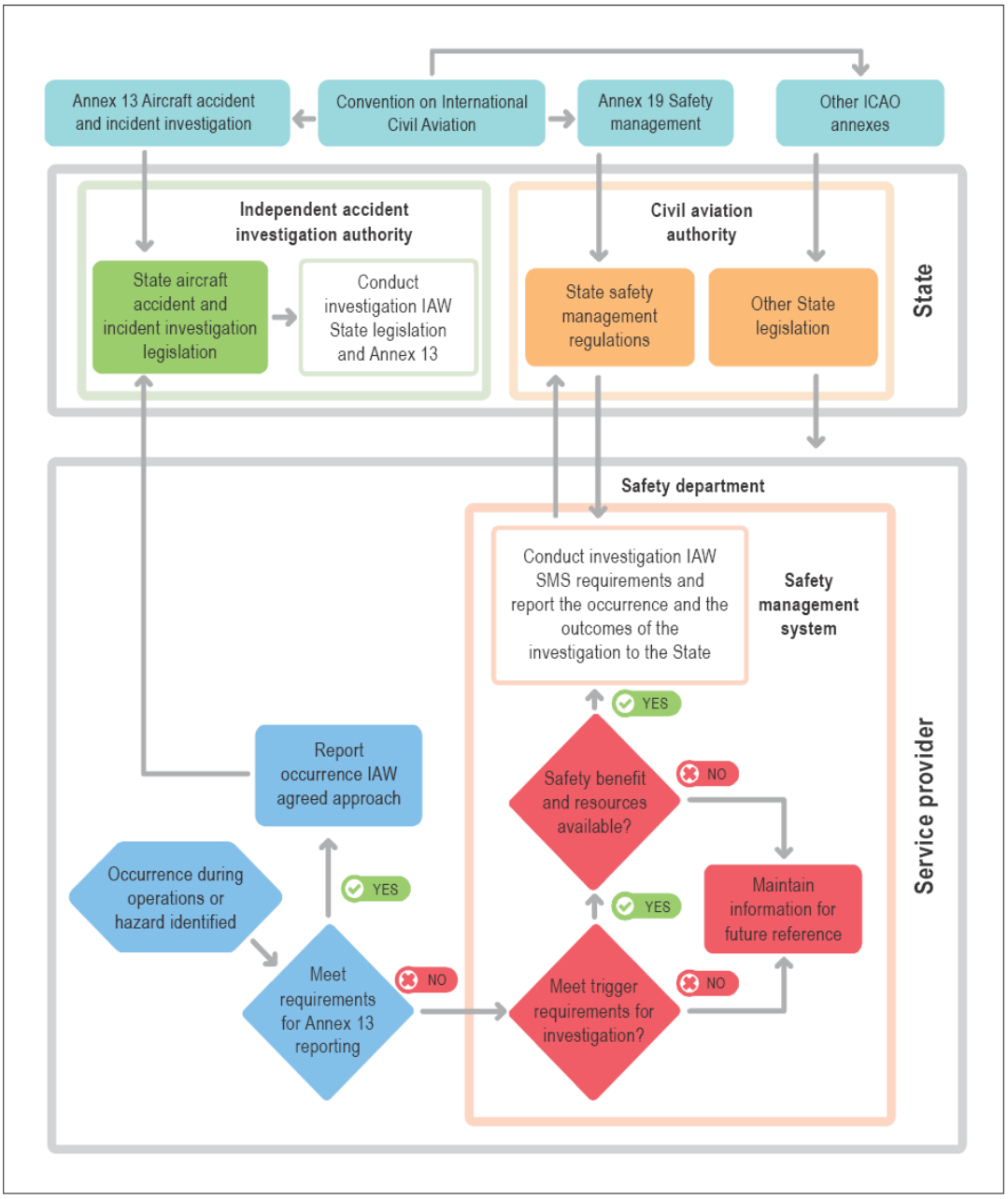

Figure 4-2. Safety investigation decision process

4.2.8.3. The investigation process

The investigation aims at identifying what happened and why it happened and this may require root cause analysis to be applied as part

of the investigation. Ideally, the people involved in the event should be interviewed as soon as possible after the event. The investigation should include:

a) establishing timelines of key events, including the actions of the people involved;
b) review of any policies and procedures related to the activities;
c) review of any decisions made related to the event;
d) identifying any risk controls that were in place that should have prevented the event occurring; and
e) reviewing safety data for any previous or similar events.

The safety investigation must focus on the identified hazards and safety risks and opportunities for improvement, not on blame or punishment. The way the investigation is conducted, and most importantly, how the report is written, will influence the likely safety impact, the future safety culture of the organization, and the effectiveness of future safety initiatives. The investigation must conclude with clearly defined findings and recommendations that eliminate or mitigate safety deficiencies.

4.3. Safety risk assessment and mitigation

The service provider must develop a safety risk assessment model and procedures which will allow a consistent and systematic approach for the assessment of safety risks. This must include a method that will help determine the consequences of identified hazards, the safety risks, what safety risks are acceptable or unacceptable and to prioritize actions.

4.3.1. Consequences of hazards

The service provider shall develop and maintain a formal process to identify consequences of hazards that have been identified to possibly impact aviation safety in the operation and activities.

The SRM tools used may need to be reviewed and customized periodically to ensure they are suitable for the service provider's operating environment. The service provider may find more sophisticated approaches that better reflect the needs of their operation as their SMS matures. The methodology shall be submitted to the Authority for approval.

The safety risk assessment process shall use whatever safety data and safety information is available. Once safety risks have been assessed, the service provider will engage in a data-driven decision-making process to determine what safety risk controls are needed.

Safety risk assessments may also use qualitative information (expert judgment) rather than quantitative data due to unavailability of data. Using the safety risk matrix allows the user to express the safety risk(s) associated with the identified hazard in a quantitative format. This enables direct magnitude comparison between identified safety risks. A qualitative safety risk assessment criterion such as “likely to occur” or “improbable” may be assigned to each identified safety risk where quantitative data is not available.

For service providers that have operations in multiple locations with specific operating environments, it may be more effective to establish local safety committees to conduct safety risk assessments and safety risk control identification. Advice may also be sought from a specialist in the operational area (internal or external to the service provider).

4.3.2. Safety risk probability

The service provider’s risk assessment model and procedures shall include an evaluation of the safety risk probability which is defined as the likelihood that a safety consequence or outcome will occur. It is important to envisage a variety of scenarios so that all potential consequences can be considered. The following questions can assist in the determination of probability:

a) Is there a history of occurrences similar to the one under consideration, or is this an isolated occurrence?
b) What other equipment or components of the same type might have similar issues?
c) What is the number of personnel following, or subject to, the procedures in question?
d) What is the exposure of the hazard under consideration? For example, during what percentage of the operation is the equipment or activity in use?

Taking into consideration any factors that might underlie these questions will help when assessing the probability of the hazard consequences in any foreseeable scenario.

An occurrence is considered foreseeable if any reasonable person could have expected the kind of occurrence to have happened under the same circumstances. Identification of every conceivable or theoretically possible hazard is not possible. Therefore, good judgment is required to determine an appropriate level of detail in hazard identification. Service providers should exercise due diligence when identifying significant and reasonably foreseeable hazards related to their product or service.

Table 4-1 presents a typical safety risk probability classification table that may be adopted by services providers in the assignment of the

probability of safety risks. It includes five categories to denote the probability related to an unsafe event or condition, the description of each category, and an assignment of a value to each category.

Likelihood	*Meaning*	*Value*
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

Table 4-1 Safety risk probability table

4.3.3. Safety risk severity

The service provider's risk assessment model and procedures shall include an assessment of the safety risk severity which is defined as the extent of harm that might reasonably be expected to occur as a consequence or outcome of the identified hazard.

The assessment of the severity must take into account the potential consequences related to the hazard, and includes considerations of :

1) fatalities or serious injury which would occur as a result of:
   a) being in the aircraft;
   b) having direct contact with any part of the aircraft, including parts which have become detached from the aircraft; or
   c) having direct exposure to jet blast; and
2) damage:
   a) damage or structural failure sustained by the aircraft which:
      i) adversely affects the structural strength, performance or flight characteristics of the aircraft;
      ii) would normally require major repair or replacement of the affected component;
   b) damage sustained by ATS or aerodrome equipment which:
      i) adversely affects the management of aircraft separation; or
      ii) adversely affects landing capability.

The severity assessment shall consider all possible consequences related to a hazard, taking into account the worst foreseeable situation. Table 4-2 presents a typical safety risk severity table that may be adopted by services providers in the assignment of the severity of safety risks. It includes five categories to denote the level of severity, the description of each category, and the assignment of a value to each category.

severity	*Meaning*	*Value*
Catastrophic	• Aircraft / equipment destroyed • Multiple deaths	A
Hazardous	• A large reduction in safety margins, physical distress or a workload such that operational personnel cannot be relied upon to perform their tasks accurately or completely • Serious injury • Major equipment damage	B
Major	• A significant reduction in safety margins, a reduction in the ability of operational personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency • Serious incident • Injury to persons	C
Minor	• Nuisance • Operating limitations • Use of emergency procedures • Minor incident	D
Negligible	Few consequences	E

Table 4-2 Safety risk severity table

4.3.4. Safety risk tolerability

The service provider's risk assessment model and procedures shall include a safety risk index rating that is created by combining the results of the probability and severity scores. The respective severity/probability combinations are presented in the safety risk assessment matrix in Table 4-3. The safety risk assessment matrix shall be used to determine safety risk tolerability.

Safety risk	Severity				
Probability	Catastrophic	Hazardous	Major	Minor	Negligible
Frequent	5A	5B	5C	5D	5E
Occasional	4A	4B	4C	4D	4E
Remote	3A	3B	3C	3D	3E
Improbable	2A	2B	2C	2D	2E
Extremely improbable	1A	1B	1C	1D	1E

Table 4-3 Safety risk matrix

The index obtained from the safety risk assessment matrix shall then be exported to a safety risk tolerability table that describes — in a narrative form — the tolerability criteria for the service provider. Table 4-4 presents a safety risk tolerability table.

Safety risks are conceptually assessed as acceptable, tolerable or intolerable:

1) safety risks assessed as initially falling in the intolerable region are unacceptable under any circumstances. The probability and/or severity of the consequences of the hazards are of such a magnitude, and the damaging potential of the hazard poses such a threat to safety, In this case, the service provider is required to take risk control action to reduce:
   a) its exposure to the particular risk, i.e., reduce the probability component of the risk to an acceptable level;
   b) the severity of consequences related to the hazard, i.e., reduce the severity component of the risk to an acceptable level; or
   c) both the severity and probability so that the risk is managed to an acceptable level.
2) safety risks assessed as initially falling in the tolerable region can be tolerated based on the safety risk mitigation.
3) safety risks assessed as initially falling in the acceptable are acceptable as is.

Table 4-4 presents an example of a safety risk tolerability table that may be adopted by a service provider.

Safety Index range	Safety risk description	Recommended action
5A, 5B, 5C, 4A, 4B, 3A	INTOLERABLE	Take immediate action to mitigate the risk or stop the activity. Perform priority safety risk mitigation to ensure additional or enhanced preventative controls are in place to bring down the safety risk index to tolerable.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	TOLERABLE	Can be tolerated based on the safety risk mitigation. It may require management decision to accept the risk.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACCEPTABLE	Acceptable as is. No further safety risk mitigation required.

Table 4-4 Safety risk tolerability

4.3.5. Assessing human factors related risks

The consideration of human factors has particular importance in SRM as people can be both a source and a solution of safety risks by:

a) contributing to an accident or incident through variable performance due to human limitations;
b) anticipating and taking appropriate actions to avoid a hazardous situation: and
c) solving problems, making decisions and taking actions to mitigate risks.

The implementation of service provider's risk assessment model and procedures shall involve people with appropriate human factors expertise in the identification, assessment and mitigation of risks to ensure that all aspects of safety risk are addressed, including those related to humans.

4.3.6. Safety risk mitigation strategies

The service provider's risk assessment model and procedures shall include the identification of safety risk mitigation or safety risk control to manage the identified safety risks to an acceptable level. This should be balanced against the time, cost and difficulty of taking action to reduce or eliminate the safety risk. The level of safety risk can be lowered by reducing the severity of the potential consequences, reducing the likelihood of occurrence or by reducing exposure to that safety risk. It is easier and more common to reduce the likelihood than it is to reduce the severity.

Safety risk mitigations are actions that often result in changes to operating procedures, equipment or infrastructure. Safety risk mitigation strategies fall into three categories:

a) *Avoidance*: The operation or activity is cancelled or avoided because the safety risk exceeds the benefits of continuing the activity, thereby eliminating the safety risk entirely.

b) Reduction: The frequency of the operation or activity is reduced, or action is taken to reduce the magnitude of the consequences of the safety risk.

c) Segregation: Action is taken to isolate the effects of the consequences of the safety risk or build in redundancy to protect against them.

The consideration of human factors is an integral part of identifying effective mitigations because humans are required to apply, or contribute to, the mitigation or corrective actions. For example, mitigations may include the use of processes or procedures. Without input from those who will be using these in "real world" situations and/or individuals with human factors expertise, the processes or procedures developed may not be fit for their purpose and result in unintended consequences. Further, human performance limitations must be considered as part of any safety risk mitigation, building in error capturing strategies to address human performance variability. Ultimately, this important human factors perspective results in more comprehensive and effective mitigations.

A safety risk mitigation strategy may involve one of the approaches described above or may include multiple approaches. It is important to consider the full range of possible control measures to find an optimal solution.

The effectiveness of each alternative strategy must be evaluated before a decision is made. Each proposed safety risk mitigation alternative shall be examined from the following perspectives:

a) *Effectiveness*. The extent to which the alternatives reduce or eliminate the safety risks. Effectiveness can be determined in terms of the technical, training and regulatory defences that can reduce or eliminate safety risks.
b) *Cost/benefit*. The extent to which the perceived benefits of the mitigation outweighs the costs.
c) *Practicality*. The extent to which mitigation can be implemented and how appropriate it is in terms of available technology, financial and administrative resources, legislation, political will, operational realities, etc.
d) *Acceptability*. The extent to which the alternative is acceptable to those people that will be expected to apply it.
e) *Enforceability*. The extent to which compliance with new rules, regulations or operating procedures can be monitored.
f) *Durability*. The extent to which the mitigation will be sustainable and effective.
g) *Residual safety risks*. The degree of safety risk that remains subsequent to the implementation of the initial mitigation and which may necessitate additional safety risk control measures.
h) *Unintended consequences*. The introduction of new hazards and related safety risks associated with the implementation of any mitigation alternative.
i) *Time*. Time required for the implementation of the safety risk mitigation alternative.

4.3.7. Implementation of safety risk mitigation strategies

Final decisions or control acceptance may be required from higher authorities so that the appropriate resources are provided.

How service providers go about prioritizing their safety risk assessments and adopting safety risk controls is their decision. As a guide, the service provider should find the prioritization process:

a) assesses and controls highest safety risk;
b) allocates resources to highest safety risks;
c) effectively maintains or improves safety;
d) achieves the stated and agreed safety objectives and SPTs; and
e) satisfies the requirements of the Authority's regulations with regard to control of safety risks.

After safety risks have been assessed, appropriate safety risk controls can be implemented. It is important to involve the “end users” and subject matter experts in determining appropriate safety risk controls. Ensuring the right people are involved will maximize the practicality of safety risk chosen mitigations. A determination of any unintended

consequences, particularly the introduction of new hazards, should be made prior to the implementation of any safety risk controls.

Once the safety risk control has been agreed and implemented, the safety performance must be monitored to assure the effectiveness of the safety risk control. This is necessary to verify the integrity, efficiency and effectiveness of the new safety risk controls under operational conditions.

4.4. Safety risk management documentation

The SRM outputs must be documented including any assumptions underlying the probability and severity assessment, decisions made, and any safety risk mitigation actions taken.

Services provider are required to include in the implementation of their SMS a safety data collection and processing system (SDCPS) where large amounts of safety data and safety information can be stored and analysed. The SDCPS must include the hazard and any consequences, the safety risk assessment and any safety risk control actions taken. These must be captured in a register so they can be tracked and monitored. When hazards are identified, they can be compared with the known hazards in the register to see if the hazard has already been registered, and what action(s) were taken to mitigate it. The hazard register must include: the hazard, potential consequences, assessment of associated risks, identification date, hazard category, short description, when or where it applies, who identified it and what measure have been put in place to mitigate the risks.

This SRM documentation becomes a historical source of organizational safety knowledge which can be used as reference when making safety decisions and for safety information exchange. This safety knowledge provides material for safety trend analyses and safety training and communication. It shall also include tools to assess whether safety risk controls and actions have been implemented and are effective.

Safety risk decision-making tools and processes can be used to improve the repeatability and justification of decisions taken by organizational safety decision makers. An example of a safety risk decision aid is provided below in Figure 4-3.

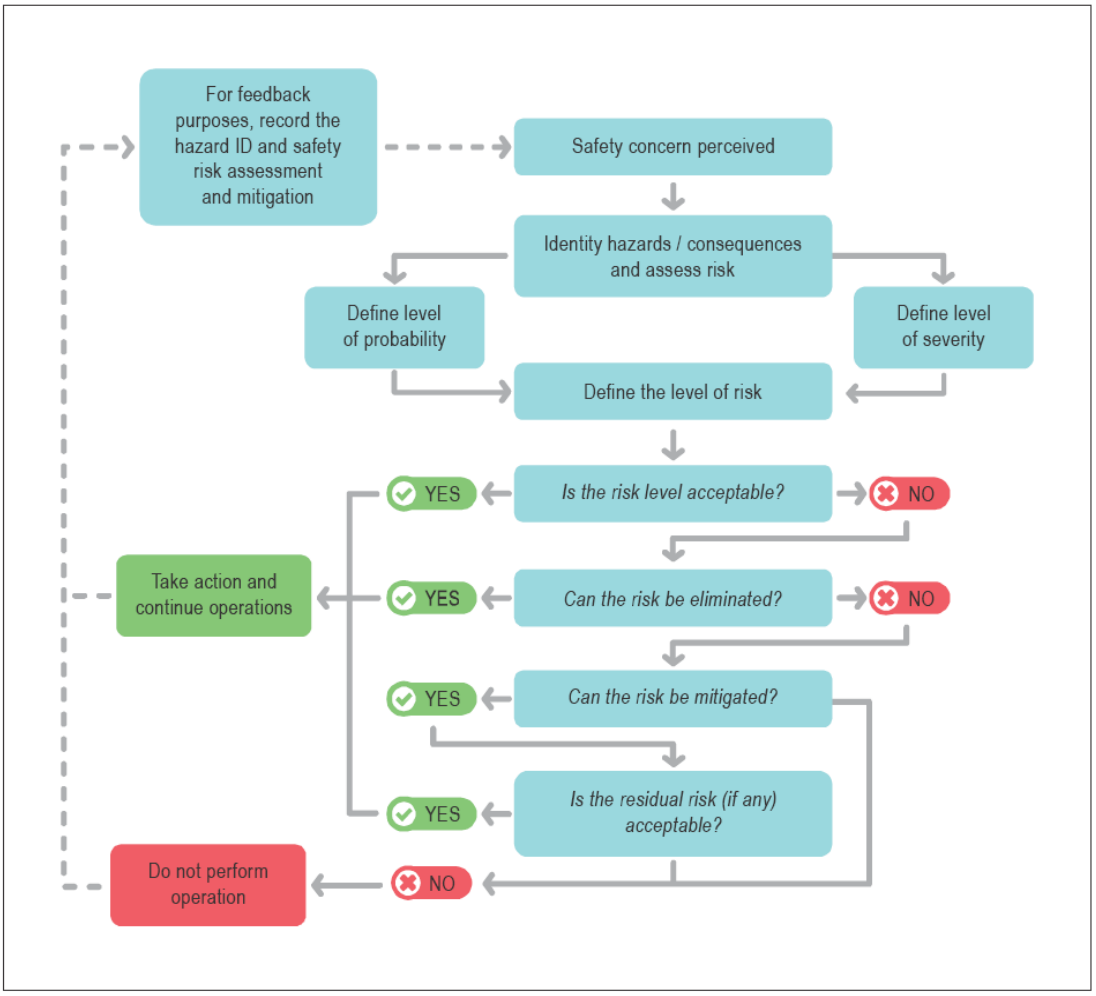

Figure 4-3 : Safety risk management decision aid

Chapter 5 – Safety Assurance

5.1. General

Safety assurance consists of processes and activities undertaken to determine whether the SMS is operating according to expectations and requirements. This involves continuously monitoring its processes as well as its operating environment to detect changes or deviations that may introduce emerging safety risks or the degradation of existing safety risk controls.

The safety assurance activities must also include the development and implementation of actions taken in response to any identified issues having a potential safety impact.

5.2. Safety performance monitoring and measurement

To verify the safety performance and validate the effectiveness of safety risk controls, the service provider will make use of a combination of internal audits and the establishment and monitoring of SPIs.

5.2.1. Internal audit

5.2.1.1. Objectives of the internal audit

The service provider's SMS shall include a procedure of internal audits to:

a) assess the effectiveness of the SMS,
b) identify areas for potential improvement,
c) ensure that any safety risk controls are effectively implemented and monitored, and
d) investigate and analyse the causes and contributing factors where non-conformances and other issues are identified.

5.2.1.2. Focus of the internal audit

The main focus of the internal audit is on the policies, processes and procedures that provide the safety risk controls with the aim to provide the accountable executive and senior management with feedback on the status of:

a) compliance with regulations;
b) compliance with policies, processes and procedures;
c) the effectiveness of safety risk controls;
d) the effectiveness of corrective actions;
e) progress in closing previously identified non-compliances ;and
f) the effectiveness of the SMS.

5.2.1.3. Description and content of the internal audit procedure

The description of the internal audit shall include least the following:

a) Audit system;

b) Auditors;
c) Monitoring and corrective action;
d) Management evaluation;
e) Feedback to the SRM; and
f) Integration of inputs from second- and third-party audits.

5.2.1.4. Audit system

The internal audit shall include an audit system that consists of the following:

a) an initial audit conducted within 12 months after the issue of the acceptance of the SMS;
b) an audit of the entire SMS carried out every three years, calculated from the initial audit, in one of the following ways:
   i. a complete audit, or
   ii. a series of audits conducted at intervals set out in SMS manual;
c) checklists of all activities controlled by the SMS manual;
d) a record of each occurrence of non-compliance or non-effectiveness during an audit referred to in paragraph (a) or (b);
e) procedures for ensuring that each finding of an audit is communicated to the accountable executive;
f) follow-up procedures for ensuring that corrective actions are effective; and
g) a system for recording the findings of an audit referred to in paragraph (a) or (b), corrective actions and follow-ups.

The checklists referred to in (c) may include questions to assess compliance and effectiveness of each process or procedure:

1) Determining compliance
   a) Does the required process or procedure exist?
   b) Is the process or procedure documented (inputs, activities, interfaces and outputs defined)?
   c) Does the process or procedure meet requirements (criteria)?
   d) Is the process or procedure being used?
   e) Are all affected personnel following the process or procedure consistently?
   f) Are the defined outputs being produced?
   g) Has a process or procedure change been documented and implemented?
2) Assessing effectiveness
   a) Do users understand the process or procedure?
   b) Is the purpose of the process or procedure being achieved consistently?
   c) Are the results of the process or procedure what the “customer” asked for?
   d) Is the process or procedure regularly reviewed?

e) Is a safety risk assessment conducted when there are changes to the process or procedure?
f) Have process or procedure improvements resulted in the expected benefits?

5.2.1.5. Auditors

The internal audit procedure shall document the process of appointment of auditors, their responsibilities of the auditors, to include as a minimum:

a) Perform audits as part of the internal audit;
b) Identify and record any concerns or findings, and the evidence necessary to substantiate such concerns or findings;
c) Initiate or recommend solutions to concerns or findings through designated reporting channels;
d) Verify the implementation of solutions within specific timescales; and
e) Report directly to the person responsible for the management of the internal audit.

The service provider should decide, depending upon the complexity of the operations, whether to make use of a dedicated audit team or a single auditor. In any event, the auditor or audit team should have relevant operational and/or maintenance experience.

5.2.1.6. Audits findings

The internal audit procedure shall include arrangements for records relating to the findings resulting from the audit system to be distributed to the appropriate manager for corrective action and follow-up in accordance with the policies and procedures specified in the service provider's document management system.

5.2.1.7. Records of findings

The records of the audits findings shall be retained for the greater of

a) two audit cycles, and
b) two years.

5.2.1.8. Corrective actions

The internal audit procedure shall include arrangements to ensure that subsequent to an audit, the service provider establishes:

a) The seriousness of any findings and any need for immediate corrective action;
b) The origin of the finding;
c) What corrective actions are required to ensure that the non-compliance does not recur;
d) A schedule for corrective action;
e) The identification of individuals or departments responsible for implementing corrective action;

5.2.1.9. Management evaluation

The internal audit procedure shall include arrangements to ensure that subsequent to an audit, the audit reports are forwarded to the safety manager, SAGs, and SRB, as appropriate, in order to:

a) allocate resources, where appropriate,
b) ensure that corrective action is taken by the manager responsible in response to any finding of noncompliance;
c) monitor the implementation and completion of corrective action; and
d) provide management with an independent assessment of corrective action; implementation and completion.

5.2.1.10. Feedback to the SRM

The description of the internal audit shall include a process to take into account the results of the internal audit as one of the various inputs to the SRM and safety assurance functions. This shall include hw the internal audit inform the service provider's management of the level of compliance within the organization, the degree to which safety risk controls are effective and where corrective or preventive action is required.

5.2.1.11. Integration of results of second and third-party audits

The Authority may provide additional feedback on the status of compliance with regulations, and the effectiveness of the SMS and industry associations or other third parties selected by the service provider to audit their organization and processes. Results of such second- and third-party audits are inputs to the safety assurance function, providing the service provider with indications of the effectiveness of their internal audit processes and opportunities to improve their SMS.

The description of the internal audit shall include a process to integrate input from such second-and third party audits into the internal auditing system.

5.2.2. Safety performance monitoring

5.2.2.1. Safety objectives, SPIs, and SPTs

The service provider shall define:

1) safety objectives, established first to reflect the strategic achievements or desired outcomes related to safety concerns specific to the service provider's operational context;
2) SPIs, which are tactical parameters related to the safety objectives and therefore are the reference for data collection, encompassing a wide spectrum of indicators:
   a) low probability/high severity events (e.g. accidents and serious incidents);

b) high probability/low severity events (e.g. uneventful operational events, non-conformance reports, deviations etc.); and
c) process performance (e.g. training, system improvements and report processing); and

3) SPTs, which are also tactical parameters used to monitor progress towards the achievement of the safety objectives.

During development of SPIs and SPTs, the service provider must consult with the Authority.

5.2.2.2. Establishment of safety objectives

Safety objectives must be established as brief, high-level statements of safety achievements or desired outcomes to be accomplished. Safety objectives provide direction to the service provider's activities and must therefore be consistent with the safety policy that sets out the service provider's high-level safety commitment. Safety objectives may be:

a) *process-oriented*: stated in terms of safe behaviours expected from operational personnel or the performance of actions implemented by the organization to manage safety risk; or
b) *outcome-oriented*: encompass actions and trends regarding containment of accidents or operational losses.

The suite of safety objectives shall include a mix of both process-oriented and outcome-oriented objectives to provide enough coverage and direction for the SPIs and SPTs.

Process oriented	Increase safety reporting levels
Outcome oriented	Reduce rate of adverse apron safety events. (high-level) or Reduce the annual number of adverse apron safety events from the previous year.

Table 5-1 Examples of safety objectives

5.2.2.3. Establishment of SPIs

The development of SPIs shall be linked to the safety objectives and be based on the analysis of data that is available or obtainable. SPIs are used to help senior management know whether or not the organization is likely to achieve its safety objective; they can be qualitative or quantitative.

Quantitative indicators relate to measuring by the quantity, rather than its quality, whereas qualitative indicators are descriptive and measure by quality. Quantitative indicators where appropriate, shall be reflected in terms of a relative rate to measure the performance level regardless of the level of activity.

Quantitative indicators are preferred over qualitative indicators because they are more easily counted and compared. The choice of indicator depends on the availability of reliable data that can be measured quantitatively. Does the necessary evidence have to be in the form of comparable, generalizable data (quantitative) or a descriptive image of the safety situation (qualitative)?

Each option, qualitative or quantitative, involves different kinds of SPIs, and requires a thoughtful SPI selection process.

A combination of approaches is useful in many situations, and can solve many of the problems which may arise from adopting a single approach.

The two most common categories of SPIs are lagging and leading.

1) Lagging SPIs measure events that have already occurred. They are also referred to as “outcome-based SPIs” or “activity or process SPIs” as they monitor and measure conditions that have the potential to lead to or contribute to a specific outcome. Lagging SPIs are divided into two types:
   a) *low probability/high severity*: outcomes such as accidents or serious incidents. The low frequency of high severity outcomes means that aggregation of data (at industry segment level or regional level) may result in more meaningful analyses. An example of this type of lagging SPI would be “aircraft and/or engine damage due to bird strike”.
   b) *high probability/low severity*: outcomes that did not necessarily manifest themselves in a serious accident or incident, these are sometimes also referred to as precursor indicators. SPIs for high probability/low severity outcomes are primarily used to monitor specific safety issues and measure the effectiveness of existing safety risk mitigations. An example of this type of precursor SPI would be “bird radar detections”, which indicates the level of bird activity rather than the amount of actual bird strikes.
2) Leading indicators are measures that focus on processes and inputs that are being implemented to improve or maintain safety. These are also known as “activity or process SPIs” as they monitor and measure conditions that have the potential to become or to contribute to a specific outcome. Examples of leading SPIs driving the development of organizational capabilities for proactive safety performance management include such things as “percentage of staff who have successfully completed safety training on time” or “frequency of bird scaring activities”. Leading SPIs may also inform the organization about how their operation copes with change, including changes in its operating environment. The focus will be

either on anticipating weaknesses and vulnerabilities as a result of the change, or monitoring the performance after a change. An example of an SPI to monitor a change in operations would be "percentage of sites that have implemented procedure X".

For a more accurate and useful indication of safety performance, lagging SPIs, measuring both "low probability/high severity" events and "high probability/low severity" events should be combined with leading SPIs.

When establishing SPIs, the service providers shall consider:

a) *Measuring the right things*: Determine the best SPIs that will show the organization is on track to achieving its safety objectives. Also consider what are the biggest safety issues and safety risks faced by the organization, and identify SPIs which will show effective control of these.
b) *Availability of data*: Is there data available which aligns with what the organization wants to measure? If there isn't, there may be a need to establish additional data collection sources. For small organizations with limited amounts of data, the pooling of data sets may also help to identify trends. This may be supported by industry associations who can collate safety data from multiple organizations.
c) *Reliability of the data*: Data may be unreliable either because of its subjectivity or because it is incomplete.
d) *Common industry SPIs*: It may be useful to agree on common SPIs with similar organizations so that comparisons can be made between organizations. The regulator or industry associations may enable these.

5.2.2.4. Defining SPIs

The SPIs shall be:

a) related to the safety objective they aim to indicate;
b) selected or developed based on available data and reliable measurement;
c) appropriately specific and quantifiable; and
d) realistic, by taking into account the possibilities and constraints of the service provider.

The contents of each SPI shall include:

a) a description of what the SPI measures;
b) the purpose of the SPI (what it is intended to manage and who it is intended to inform);
c) the units of measurement and any requirements for its calculation;

d) who is responsible for collecting, validating, monitoring, reporting and acting on the SPI (these may be staff from different parts of the organization);
e) where or how the data should be collected; and
f) the frequency of reporting, collecting, monitoring and analysis of the SPI data.

5.2.2.5. Use of SPIs

The SPIs shall be used to measure operational safety performance of the service provider and the performance of their SMS. SPIs rely on the monitoring of data and information from various sources including the safety reporting system. They shall be specific to the individual service provider and be linked to the safety objectives already established.

5.2.2.6. SPTs

Once SPIs have been established the service provider shall identify SPTs.

Safety performance targets (SPTs) define short-term and medium-term safety performance management desired achievements. They act as “milestones” that provide confidence that the organization is on track to achieving its safety objectives and provide a measurable way of verifying the effectiveness of safety performance management activities. SPT setting shall take into consideration factors such as the prevailing level of safety risk, safety risk tolerability, as well as expectations regarding the safety of the particular aviation sector. The setting of SPTs shall be determined after considering what is realistically achievable for the associated aviation sector and recent performance of the particular SPI, where historical trend data is available.

SPTs shall be realistic, context specific and achievable when considering the resources available to the organization and the associated aviation sector.

5.2.2.7. Safety riggers or alert levels

The service provider shall establish triggers or alert levels as levels or criterion values that serves to trigger (start) an evaluation, decision, adjustment or remedial action related to the particular indicator. One method for setting out-of-limits trigger criteria for SPTs is the use of the population standard deviation (STDEVP) principle. This method derives the standard deviation (SD) value based on the preceding historical data points of a given safety indicator. The SD value plus the average (mean) value of the historical data set forms the basic trigger value for the next monitoring period. The SD principle (a basic statistical function) sets the trigger level criteria based on actual historical performance of the given

indicator (data set), including its volatility (data point fluctuations). A more volatile historical data set will usually result in a higher (more generous) trigger level value for the next monitoring period. Triggers provide early warnings which enable decision makers to make informed safety decisions, and thus improve safety performance. An example of trigger levels based on standard deviations (SDs) is provided at Figure 5-1 below. In this example, data-driven decisions and safety mitigation actions may need to be taken when the trend goes beyond +1SD or +2SD from the mean of the preceding period. Often the trigger levels (in this case +1SD, +2SD or beyond +2SD) will align with decision management levels and urgency of action.

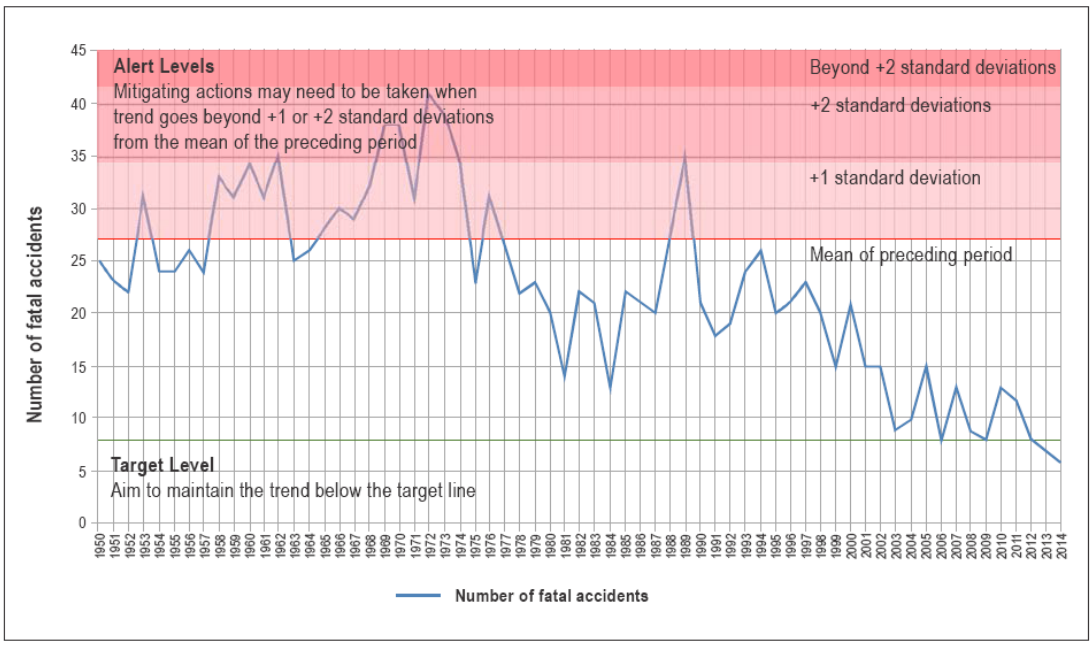

Figure 5-1 Example of representation of safety triggers (alert) levels

5.2.3. Monitoring and measuring safety performance

The service provider shall establish and document procedures for monitoring and measuring safety performance. The monitoring and measurement process involves the use of selected safety performance indicators, corresponding SPTs and safety triggers.

The service provider shall monitor the performance of established SPIs and SPTs to identify abnormal changes in safety performance. Primarily, safety performance monitoring and measurement provides a means to verify the effectiveness of safety risk controls. In addition, they provide a measure of the integrity and effectiveness of SMS processes and activities.

The following activities can provide sources to monitor and measure safety performance:

a) *Safety studies* are analyses to gain a deeper understanding of safety issues or better understand a trend in safety performance.
b) *Safety data analysis* uses the safety reporting data to uncover common issues or trends that might warrant further investigation.
c) *Safety surveys* examine procedures or processes related to a specific operation. Safety surveys may involve the use of checklists, questionnaires and informal confidential interviews. Safety surveys generally provide qualitative information. This may require validation via data collection to determine if corrective action is required. Nonetheless, surveys may provide an inexpensive and valuable source of safety information.
d) *Safety audits* focus on assessing the integrity of the service provider's SMS and supporting systems.
e) *Operational data collection systems* such as FDA, radar information can provide useful data of events and operational performance.
f) *Findings and recommendations from safety investigations* can provide useful safety information that can be analysed against other collected safety data.

5.2.4. Update of Safety Objectives

The service provider shall establish procedure for the review and update of its safety performance management:

a) routinely, in accordance with the periodic cycle established and agreed upon by the high-level safety committee;
b) based on inputs from safety analyses; and
c) in response to major changes in the operation, top risks or environment.

The set of SPIs and SPTs selected by an organization shall be periodically reviewed to ensure their continued meaningfulness as indications of organizational safety performance. Some reasons to continue, discontinueor change SPIs and SPTs include:

a) SPIs continually report the same value (such as zero per cent or 100 per cent); these SPIs are unlikely to provide meaningful input to senior management decision-making;
b) SPIs that have similar behaviour and as such are considered a duplication;
c) the SPT for an SPI implemented to measure the introduction of a programme or targeted improvement has been met;
d) another safety concern becomes a higher priority to monitor and measure;
e) to gain a better understanding of a particular safety concern by narrowing the specifics of an SPI (i.e. reduce the "noise" to clarify the "signal"); and

f) safety objectives have changed and as a consequence the SPIs require updating to remain relevant.

5.3. The management of change

The service provider shall establish a procedure for managing changes that it may experience due to a number of factors including, but not limited to:

a) organizational expansion or contraction;
b) business improvements that impact safety; these may result in changes to internal systems,
c) processes or procedures that support the safe delivery of the products and services;
d) changes to the organization's operating environment;
e) changes to the SMS interfaces with external organizations; and
f) external regulatory changes, economic changes and emerging risks.

Change may affect the effectiveness of existing safety risk controls. In addition, new hazards and related safety risks may be inadvertently introduced into an operation when change occurs. Hazards shall be identified and related safety risks assessed and controlled as defined in the organization's existing hazard identification or SRM procedures.

The service provider's management of change process shall take into account the following considerations:

a) Criticality. How critical is the change? The service provider should consider the impact on their organization's activities, and the impact on other organizations and the aviation system.
b) Availability of subject matter experts. It is important that key members of the aviation community are involved in the change management activities; this may include individuals from external organizations.
c) Availability of safety performance data and information. What data and information is available that can be used to give information on the situation and enable analysis of the change?

The management of change shall include a regular review of the system description should be to determine its continued validity, given that most service providers experience regular, or even continuous, change.

The service provider shall define the trigger for the formal change process. Changes that are likely to trigger formal change management include:

a) introduction of new technology or equipment;
b) changes in the operating environment;
c) changes in key personnel;

d) significant changes in staffing levels;
e) changes in safety regulatory requirements;
f) significant restructuring of the organization; and
g) physical changes (new facility or base, aerodrome layout changes etc.).

The change management process shall include the following activities:

a) *understand and define the change;* a description of the change and why it is being implemented;
b) *understand and define who and what it will affect;* this may be individuals within the organization, other departments or external people or organizations. Equipment, systems and processes may also be impacted. A review of the system description and organizations' interfaces may be needed. This is an opportunity to determine who should be involved in the change. Changes might affect risk controls already in place to mitigate other risks, and therefore change could increase risks in areas that are not immediately obvious;
c) *identify hazards related to the change and carry out a safety risk assessment;* identification of any hazards directly related to the change. The impact on existing hazards and safety risk controls that may be affected by the change shall also be reviewed, using the existing organization's SRM processes;
d) *develop an action plan;* define what is to be done, by whom and by when, how the change will be implemented and who will be responsible for which actions, and the sequencing and scheduling of each task;
e) sign off on the change; confirm that the change is safe to implement. The individual with overall responsibility and authority for implementing the change must sign the change plan; and
f) *assurance plan;* determine what follow-up action is needed. Consider how the change will be communicated and whether additional activities (such as audits) are needed during or after the change. Any assumptions made need to be tested.

5.4. Continuous improvement of SMS

service providers shall establish and implement a variety of methods to determine its effectiveness, measure outputs as well as outcomes of the processes, and assess the information gathered through these activities. Such methods may include:

a) *Audits*; this includes internal audits and audits carried out by other organizations.
b) *Assessments*; includes assessments of safety culture and SMS effectiveness.

c) *Monitoring of occurrences*: monitor the recurrence of safety events including accidents and incidents as well as errors and rule-breaking situations.
d) *Safety surveys*; including cultural surveys providing useful feedback on staff engagement with the SMS. It may also provide an indicator of the safety culture of the organization.
e) *Management reviews*; examine whether the safety objectives are being achieved by the organization and are an opportunity to look at all the available safety performance information to identify overall trends. It is important that senior management review the effectiveness of the SMS. This may be carried out as one of the functions of the highest-level safety committee.
f) *Evaluation of SPIs and SPTs*; possibly as part of the management review. It considers trends and, when appropriate data is available, can be compared to other service providers or State or global data.
g) *Addressing lessons learnt*; from safety reporting systems and service provider safety investigations. These should lead to safety improvements being implemented.

Chapter 6 – Safety Promotion

6.1. General

Safety promotion encourages a positive safety culture and helps achieve the service provider's safety objectives through the combination of technical competence that is continually enhanced through training and education, effective communication, and information-sharing.

The service provider shall establish and implement processes and procedures that facilitate effective two-way communication throughout all levels of the organization. This should include clear strategic direction from the top of the organization and the enabling of "bottom-up" communication that encourages open and constructive feedback from all personnel.

6.2. Training and education

6.2.1. Requirements for training

SUCAR PART 19 requires that "the service provider shall develop and maintain a safety training programme that ensures that personnel are trained and competent to perform their SMS duties." It also requires that "the scope of the safety training programme be appropriate to each individual's involvement in the SMS."

The safety manager is responsible for ensuring there is a suitable safety training programme in place. This includes providing appropriate safety information relevant to specific safety issues met by the organization.

The service provider must determine who shall be trained and to what depth, and this will depend on their involvement in the SMS. Most people working in the organization have some direct or indirect relationship with aviation safety, and therefore have some SMS duties. This applies to any personnel directly involved in the delivery of products and services, and personnel involved in the organization's safety committees. Some administrative and support personnel will have limited SMS duties and will need some SMS training, as their work may still have an indirect impact on aviation safety.

6.2.2. Scope of safety training

The safety training programme must specify the content of safety training for support staff, operational personnel, managers and supervisors, senior managers and the accountable executive.

The training programme shall include initial and recurrent training requirements to maintain competencies.

Initial safety training must consider, as a minimum, the following:

a) organizational safety policies and safety objectives;
b) organizational roles and responsibilities related to safety;
c) basic SRM principles;
d) safety reporting systems;
e) the organization's SMS processes and procedures; and
f) human factors.

Recurrent safety training must focus on changes to the SMS policies, processes and procedures, and highlight any specific safety issues relevant to the organization or lessons learned.

The training programme needs to be tailored to the needs of the individual's role within the SMS. For example, the level and depth of training for managers involved in the organization's safety committees will be more extensive than for personnel directly involved with delivery of the organization's product or services. Personnel not directly involved in the operations may require only a high level overview of the organization's SMS.

There shall be specific safety training for the accountable executive and senior managers that includes the following topics:

a) specific awareness training for new accountable executives and post holders on their SMS accountabilities and responsibilities;
b) importance of compliance with national and organizational safety requirements;
c) management commitment;
d) allocation of resources;
e) promotion of the safety policy and the SMS;
f) promotion of a positive safety culture;
g) effective interdepartmental safety communication;
h) safety objective, SPTs and alert levels; and
i) disciplinary policy.

6.2.3. Training needs analysis

The service provider identifies the SMS duties of personnel and uses the information to examine the safety training programme and ensure each individual receives training aligned with their involvement with SMS.

A formal training needs analysis (TNA) is necessary to ensure there is a clear understanding of the operation, the safety duties of the personnel and the available training. The TNA will normally start by conducting an audience analysis, which includes the following steps:

a) Every one of the service provider's staff will be affected by the implementation of the SMS, but not in the same ways or to the same degree. Identify each staff grouping and in what ways they will interact with the safety management processes, inputs and outputs - in particular with safety duties. This information should be available from the position/role descriptions. Normally groupings of individuals will start to emerge that have similar learning needs. The service provider should consider whether it is valuable to extend the analysis to staff in external interfacing organizations;
b) Identify the knowledge and competencies needed to perform each safety duty and required by each staff grouping.
c) Conduct an analysis to identify the gap between the current safety skill and knowledge across the workforce and those needed to effectively perform the allocated safety duties.
d) Identify the most appropriate skills and knowledge development approach for each group with the aim of developing a training programme appropriate to each individual or group's involvement in safety management. The training programme must also consider the staff's ongoing safety knowledge and competency needs; these needs will typically be met through a recurrent training programme.

The competencies of personnel shall also be reviewed on a regular basis.

6.2.4. Management of training activities and records

The service provider shall identify the appropriate method for training delivery. The main objective is that, on completion of the training, personnel are competent to perform their SMS duties. Competent trainers are usually the single most important consideration; their commitment, teaching skills and safety management expertise will have a significant impact on the effectiveness of the training delivered.

The safety training programme shall also specify responsibilities for development of training content and scheduling as well as training and competency records management.

6.3. Safety communication

The service provider shall communicate the organization's SMS objectives and procedures to all appropriate personnel. There shall be a documented communication strategy that enables safety communication to be delivered by the most appropriate method based on the individual's role and need to receive safety related information.

This may be done through safety newsletters, notices, bulletins, briefings or training courses. The safety manager shall also ensure that lessons

learned from investigations and case histories or experiences, both internally and from other organizations, are distributed widely.

The safety communication shall cover activities, to:

a) *ensure that staff are fully aware of the SMS;* this is a good way of promoting the organization's safety policy and safety objectives.
b) *convey safety-critical information;* Safety critical information is specific information related to safety issues and safety risks that could expose the organization to safety risk. This could be from safety information gathered from internal or external sources such as lessons learned or related to safety risk controls. The service provider determines what information is considered safety critical and the timeliness of its communication.
c) *raise awareness of new safety risk controls and corrective actions;* The safety risks faced by the service provider will change over time, and whether this is a new safety risk that has been identified or changes to safety risk controls, these changes will need to be communicated to the appropriate personnel.
d) *provide information on new or amended safety procedures;* when safety procedures are updated it is important that the appropriate people are made aware of these changes.
e) *promote a positive safety culture and encourage personnel to identify and report hazards;* safety communication is two-way. It is important that all personnel communicate safety issues to the organization through the safety reporting system.
f) *provide feedback;* provide feedback to personnel submitting safety reports on what actions have been taken to address any concerns identified.

a) Service providers should consider whether any of the safety information listed above needs to be communicated to external organizations.

Chapter 7 – SMS Implementation

7.1. System description

An overview of the system description and the SMS interfaces shall be included in the SMS documentation. A system description may include a bulleted list with references to policies and procedures. A graphic depiction, such as a process flow chart or annotated organization chart, may be enough for some organizations. An organization shall use a method and format that works for that organization.

A system description serves to identify the features of the product, the service or the activity so that SRM and safety assurance can be effective.It helps to identify the organizational processes, including any interfaces, to define the scope of the SMS. This provides an opportunity to identify any gaps related to the service provider's SMS components and elements and may serve as a starting point to identify organizational and operational hazards.

Because each organization is unique, there is no "one size fits all" method for SMS implementation. It is expected that each organization will implement an SMS that works for its unique situation. Each organization must define for itself how it intends to go about fulfilling the fundamental requirements. To accomplish this, it is important that each organization prepare a system description that identifies its organizational structures, processes, and business arrangements that it considers important to safety management functions. Based on the system description, the organization shall identify or develop policy, processes, and procedures that establish its own safety management requirements.

When considering a system description, it is important to understand that a "system" is a set of things working together as parts of an interconnecting network. In an SMS, it is any of an organization's products, people, processes, procedures, facilities, services, and other aspects (including external factors), which are related to, and can affect, the organization's aviation safety activities. Often, a "system" is a collection of systems, which may also be viewed as a system with subsystems. These systems and their interactions with one another make up the sources of hazards and contribute to the control of safety risks. The important systems include both those which could directly impact aviation safety and those which affect the ability or capacity of an organization to perform effective safety management.

When an organization elects to make a significant or substantive change to the processes identified in the system description, the changes should be viewed as potentially affecting its baseline safety risk assessment. Thus, the system description must be reviewed as part of the management of change processes.

7.2. Interface management

Safety risks faced by service providers are affected by interfaces. Interfaces can be either internal (e.g. between departments) or external (e.g. other service providers or contracted services,). By identifying and managing these interfaces the service provider will have more control over any safety risks related to the interfaces. These interfaces shall be defined within the system description.

7.3. Identification of SMS interfaces

Service providers shall initially concentrate on interfaces in relation to its business activities. The identification of these interfaces shall be detailed in the system description that sets out the scope of the SMS and must include internal and external interfaces.

The objective of this review is to produce a comprehensive list of all interfaces. The rationale for this exercise is that there may be SMS interfaces which an organization is not necessarily fully aware of. There may also be interfaces where there are no formal agreements in place, such as with the power supply or building maintenance companies.

Once the SMS interfaces have been identified, the service provider shall consider their relative criticality in order to prioritize the management of the more critical interfaces, and their potential safety risks. Things to consider are:

a) what is being provided;
b) why it is needed;
c) whether the organizations involved has an SMS or another management system in place; and
d) whether the interface involves the sharing of safety data / information.

7.4. Assessing safety impact of interfaces

The service provider shall identify any hazards related to the interfaces and carry out a safety risk assessment using its existing hazard identification and safety risk assessment processes.

Based on the safety risks identified, the service provider may consider working with the other organization to determine and define an appropriate safety risk control strategy. By involving the other organization, they may be able to contribute to identifying hazards, assessing the safety risk as well as determining the appropriate safety risk control.

This collaborative effort is needed because the perception of safety risks may not be the same for each organization. The risk control could be carried out by either the service provider or the external organization. It is also important to recognize that each organization involved has the responsibility to identify and manage hazards that affect their own organization. This may mean the critical nature of the interface is different for each organization as they may apply different safety risk classifications and have different safety risk priorities (in term of safety performance, resources, time, etc.).

7.5. Managing and monitoring interfaces

The service provider is responsible for managing and monitoring the interfaces to ensure the safe provision of their services and products. This will ensure the interfaces are managed effectively and remain current and relevant.

Formal agreements are an effective way to accomplish this as the interfaces and associated responsibilities can be clearly defined. Any changes in the interfaces and associated impacts should be communicated to the relevant organizations.

It is important to establish coordination between the organizations involved in the interface, to include:

a) clarification of each organization's roles and responsibilities;
b) agreement of decisions on the actions to be taken (e.g. safety risk control actions and timescales);
c) identification of what safety information needs to be shared and communicated;
d) how and when coordination should take place (task force, regular meetings, ad hoc or dedicated meetings); and
e) agreeing on solutions that benefit both organizations but that do not impair the effectiveness of the SMS.

All safety issues or safety risks related to the interfaces shall be documented and made accessible to each organization for sharing and review.

7.6. SMS Scalability

The service provider's SMS, including the policies, processes and procedures, shall reflect the size and complexity of its organization and its activities. It shall consider:

a) the organizational structure and availability of resources;
b) size and complexity of the organization (including multiple sites and bases); and

c) complexity of the activities and the interfaces with external organizations.

The service provider shall carry out an analysis of its activities to determine the right level of resources to manage the SMS. This shall include the determination of the organizational structure needed to manage the SMS.
This would include considerations of who will be responsible for managing and maintaining the SMS, what safety committees are needed, if any, and the need for specific safety specialists.

7.7. Integration of management systems

Safety management is to be considered as part of a management system (and not in isolation). Therefore, a service provider may implement an integrated management system that includes the SMS. An integrated management system may be used to capture multiple certificates, authorizations or approvals or to cover other business management systems such as quality, security, occupational health and environmental management systems. This is done to remove duplication and exploit synergies by managing safety risks across multiple activities. For example, where a service provider holds multiple certificates it may choose to implement a single management system to cover all of its activities. The service provider should decide the best means to integrate or segregate its SMS to suit its business or organizational needs.
A typical integrated management system may include a:

a) quality management system (QMS);
b) safety management system (SMS);
c) security management system (SeMS),
d) environmental management system (EMS);
e) occupational health and safety management system (OHSMS);
f) financial management system (FMS);
g) documentation management system (DMS); and
h) fatigue risk management system (FRMS).

A service provider may choose to integrate these management systems based on their unique needs. Risk management processes and internal audit processes are essential features of most of these management systems. In addition, there may be other operational systems associated with the business activities that may also be integrated, such as supplier management, facilities management, etc.
A service provider may also consider applying the SMS to other areas that do not have a current regulatory requirement for an SMS. Service providers should determine the most suitable means to integrate or segregate their management system to suit their business model,

operating environment, regulatory, and statutory requirements as well as the expectations of the aviation community. Whichever option is taken, it must still ensure that it meets the SMS requirements.

7.8. SMS gap analysis and implementation plan

Before implementing an SMS, the service provider shall carry out a gap analysis. This compares the service provider's existing safety management processes and procedures with the SMS requirements as determined by the Authority. It is likely that the service provider already has some of the SMS functions in place. The development of an SMS shall build upon existing organizational policies and processes. The gap analysis identifies the gaps that need to be addressed through an SMS implementation plan that defines the actions needed to implement a fully functioning and effective SMS.

The SMS implementation plan shal provide a clear picture of the resources, tasks and processes required to implement the SMS. The timing and sequencing of the implementation plan may depend on a variety of factors that will be specific to each organization, such as:

a) regulatory, customer and statutory requirements;
b) multiple certificates held (with possibly different regulatory implementation dates);
c) the extent to which the SMS may build upon existing structures and processes;
d) the availability of resources and budgets;
e) interdependencies between different steps (a reporting system should be implemented before establishing a data analysis system); and
f) the existing safety culture.

The SMS implementation plan shall be developed in consultation with the accountable executive and other senior managers, and should include who is responsible for the actions along with timelines. The plan shall also address coordination with external organizations or contractors where applicable.

The SMS implementation plan may be documented in different forms, varying from a simple spread sheet to specialized project management software, but in all cases, shall clarify when each specific element of the SMS framework as defined in chapter 2 can be considered successfully implemented.The plan shall be monitored regularly and updated as necessary.

During the implementation phase, the SMS gap analysis and implementation plan are considered an integral part of the SMS documentation as defined in 3.6.

Chapter 8 – safety data collection, processing, analysis, and exchange

8.1. General

Safety data is what is initially reported or recorded as the result of an observation or measurement. It is transformed to safety information when it is processed, organized, integrated or analyzed in a given context to make it useful for management of safety. Safety information may continue to be processed in different ways to extract different meanings.

The effective management of safety is highly dependent on the effectiveness of safety data collection, analysis and overall management capabilities.

SUCAR PART 19 requires that service providers develop and maintain a formal process to collect, record, act on and generate feedback on hazards in their activities, based on a combination of reactive and proactive methods of safety data collection.

SUCAR PART 19 also requires States to establish safety data collection and processing systems (SDCPS) to capture, store, aggregate, and enable the analysis of safety data and safety information to support their safety performance management activities. The Authority has established the Sudan SDCPS to support its safety responsibilities.

Service providers are also required to develop and maintain the means to verify their safety performance with reference to their SPIs and SPTs, in support of their safety objectives by means of SDCPS. They may be based on reactive and proactive methods of safety data and safety information collection.

Services providers shall ensure they have personnel qualified to collect and store safety data, and the competencies needed to process safety data. This usually requires individuals with strong information technology skills as well as knowledge of data requirements, data standardization, data collection and storage, data governance and the ability to understand potential queries that may be needed for analysis. Additionally, the service provider shall ensure that each SDCPS has a designated custodian to apply the protection to safety data, safety information and related sources in accordance with Appendix C to SUCAR PART 19.

8.2. Safety Data and Safety Information Collection

8.2.1. Determining what to collect

Each service provider shall determine what safety data and safety information it must collect to support the safety performance management process and make safety decisions. Safety data and safety information requirements can be determined using a top-down and/or a bottom-up approach. The chosen approach can be influenced by different considerations, such as local conditions and priorities, or the need to provide the data to support the monitoring of the SPIs.

Identifying and collecting the safety data shall be aligned with the service provider's need to effectively manage safety. In some cases, the SRM process will highlight the need for additional safety data to better assess the
impact (the level of probability and severity) and determine the associated risks. Equally, the safety performance management process may highlight a need for additional information for a more comprehensive understanding of a particular safety issue or to facilitate the establishment or refinement of SPIs.
Service providers must consider taking an integrated approach to the collection of safety data that come from different sources, both internal and external. Integration allows organizations to get a more accurate view of their safety risks and the organization's achievement of its safety objectives. It is worth noting that safety data and safety information that initially seems to be unrelated, may later turn out to be critical for identifying safety issues and supporting data-driven decision-making.

It is advisable to streamline the amount of safety data and safety information by identifying what specifically supports the effective management of safety within their organization. The safety data and safety information collected should support the reliable measure of the system's performance and the assessment of known risks, as well as the identification of emerging risks, within the scope of the organization's activities. The safety data and safety information required will be influenced by the size and complexity of the organization's activities.

Figure 8-1 provides examples of typical safety data and safety information, which in many cases are already available. Coordination among departments or divisions is necessary to streamline efforts for reporting and collecting safety data to avoid duplication.

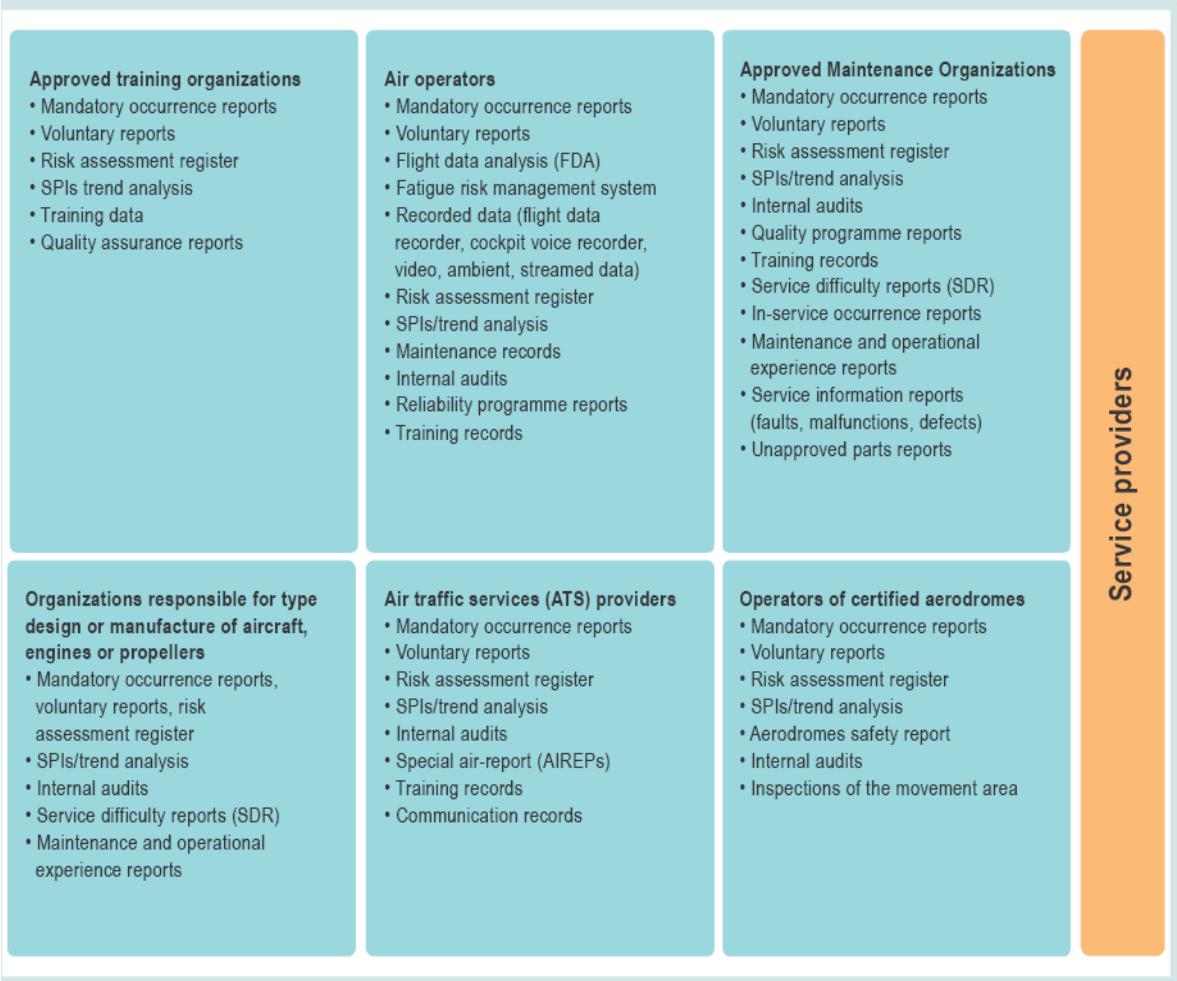

Figure 8-1 : Typical safety data and safety information sources

8.2.2. Mandatory safety reporting system

Sudan has established a mandatory safety reporting system for accidents cidents. The service providers shall establish a system to generate and submit mandatory reports as required in SUCAR PART 13. The system shall include requirements for operational personnel to report accidents and serious incidents as soon as possible and by the quickest means available to the Directorate of AAICD. The following are two main aspects to consider when deciding whether an incident should be classified as a serious incident:

a) Were there circumstances indicating that there was a high probability of an accident?
b) Was the accident avoided only due to providence?

8.2.3. Voluntary safety reporting system

Service providers shall establish a voluntary safety reporting system to collect safety data and safety information not captured by the mandatory safety reporting system.

8.2.4. Self-disclosure reporting systems

Service providers' my consider implementation of systems for the collection of safety data through self-disclosure reporting systems that capture safety data through direct observations of flight crews or air traffic controllers, including automatic data capture such as aviation safety action programme (ASAP) and FDA programmes (flight operations quality assurance (FOQA) programme, line operations safety audit (LOSA) and the normal operations safety survey (NOSS)).

8.3. Taxonomies

Safety data shall be categorized using taxonomies and supporting definitions so that the data can be captured and stored using meaningful terms. Common taxonomies and definitions establish a standard language, improving the quality of information and communication. The aviation community's capacity to focus on safety issues is greatly enhanced by sharing a common language. Taxonomies enable analysis and facilitate information sharing and exchange. Elements of taxonomies include:

a) Aircraft model: The service provider can build a database with all models certified to operate.
b) Airport: The service providers use ICAO or International Air Transport Association (IATA) codes to identify airports.
c) Type of occurrence: The service provider shall use the ADREP taxonomy to classify occurrences. It is a compilation of attributes and the related values that allow safety trend analysis on these categories.

8.4. Safety data processing

Safety data processing refers to the manipulation of safety data to produce meaningful safety information in useful forms such as diagrams, reports, or tables. The service provider shall ensure that the established SDCPS takes into account the important considerations related to safety data processing, including: data quality, aggregation, fusion, and filtering.

1) Data quality

Data quality relates to data that is clean and fit for purpose. Data quality involves the following aspects:

a) cleanliness;
b) relevance;
c) timeliness; and
d) accuracy and correctness.

Data cleansing is the process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database and refers to identifying incomplete, incorrect, inaccurate or

irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data.

Relevant data is data which meets the service provider's needs and represents their most important issues. The service provider shall assess the relevance of data based on its needs and activities. Safety data and safety information timeliness is a function of its currency. Data used for decisions shall reflect what is happening as close to real time as possible. Judgement is often required based on the volatility of the situation. For example, data collected two years ago on an aircraft type still operating the same route, with no significant changes, may provide a timely reflection of the situation. Whereas data collected one week ago on an aircraft type no longer in service may not provide a meaningful, timely reflection of the current reality.

Data accuracy refers to values that are correct and reflect the given scenario as described. Data inaccuracy commonly occurs when users enter the wrong value or make a typographical error. This problem can be overcome by having skilled and trained data entry personnel or by having components in the application such as spell check. Data values can become inaccurate over time, also known as "data decay". Movement is another cause of inaccurate data. As data is extracted, transformed and moved from one database to another, it may be altered to some extent, especially if the software is not robust.

2) Aggregation of safety data and safety information

Data aggregation is when safety data and safety information is gathered and stored in the service provider's SDCPS and expressed in a summary form for analysis. To aggregate safety data and safety information is to collect them together, resulting in a larger data set. In the case of SDCPS, individual items of safety data are aggregated into a database without giving one piece of safety data precedence over another. A common aggregation purpose is to get information about a particular group or type of activity based on specific variables such as: location; fleet type; or professional group.

Data aggregation can sometimes be helpful across multiple organizations that do not have enough data to ensure proper de-identification to protect the sources of the safety data and safety information, and to support analysis.

3) Data fusion

Data fusion is the process of merging multiple safety data sets to produce more coherent, linked and useful safety data than that provided by any individual set of safety data. The integration of safety data sets followed by its reduction or replacement improves the reliability and usability of said data.

4) Filtering of safety data and safety information

Safety data filtering refers to a wide range of strategies or solutions for y data sets. This means the data sets are refined into simply what the decision-maker needs, without including other data that can be repetitive, irrelevant or even sensitive. Different types of data filters can be used to generate reports or present the data in ways that facilitate communication.

8.5. Safety Data and Safety Information Management

Safety data and safety information management can be defined as the development, execution and supervision of plans, policies, programmes and practices that ensure the overall integrity, availability, usability, and protection of the safety data and safety information used by the service provider.

The service provider will ensure that a safety data and safety information management is in place addressing the necessary functions to ensure that the organization's safety data and safety information is collected, stored, analysed, retained and archived, as well as governed, protected and shared, as intended. Specifically, it must identify:

a) what data will be collected;
b) data definitions, taxonomy and formats;
c) how the data will be collected, collated and integrated with other safety data and safety information sources;
d) how the safety data and safety information will be stored, archived and backed up; for example, database structure, and, if an IT system, supporting architecture;
e) how the safety data and safety information will be used;
f) how the information is to be shared and exchanged with other parties;
g) how the safety data and safety information will be protected, specific to the safety data and safety information type and source; and
h) how quality will be measured and maintained.

8.6. Data governance

The service provider will establish a data governance system specifying the authority, control and decision-making over the processes and procedures that support an its data management activities. The governance dictates how safety data and safety information are collected, analysed, used, shared and protected to ensure that the data management system(s) has the desired effect through the key characteristics of integrity, availability, usability and protection as described below.

Integrity — Data integrity refers to the reliability of the sources, information, ontains. However, data integrity includes the maintenance and the assurance of the accuracy and consistency of data over its entire life-cycle. This is a critical aspect to the design, implementation and usage of the SDCPS when storing, processing, or retrieving the data.

Availability — It should be clear who has permission to use or share the stored safety data and safety information. This has to take into account the agreement between the data/information owner and custodian. For the entities that are allowed to use the data, it should be clear how to gain access and how to process it. A variety of techniques exist to maximize data availability, including redundancy of storage locations and data access methods and tools.

Usability — In order to maximize returns on safety data and safety information, it is important to also consider usability standards. Humans are continuously interacting and engaging with safety data and safety information as they are acquired. Organizations should minimize human error as automation applications are applied. Tools which can increase usability include data dictionaries and metadata repositories. As human interaction evolves towards big data applications and machine learning processes,

it will become increasingly important to better understand human usability as it is applied to machines to minimize safety data and safety information miscalculations in the future.

Protection — Services providers must ensure that safety data, safety information and related sources are afforded appropriate protection as established by the Authority.

8.7. Metadata management

Metadata is defined as a set of data that describes and gives information about other data, in other words, data about data. Using metadata standards provides a common meaning or definition of the data. It ensures proper use and interpretation by owners and users, and that data is easily retrieved for analysis.

The service provider must catalogue its data based on its properties, including but not limited to:

a) what the data is;
b) where it comes from (the original source);

c) who created it;
d) when it was created;
e) who used it;
f) what it was used for;
g) frequency of collection; and
h) any processing or transformation.

8.8. Safety Analysis

Safety analysis is the process of applying statistical or other analytical techniques to check, examine, describe, transform, condense, evaluate and visualize safety data and safety information in order to discover useful information, suggest conclusions and support data-driven decision-making.

Services providers are required to establish and maintain a process to analyse the safety data and safety information from the SDCPS and associated safety databases.

1) Types of analysis

Common approaches include descriptive analysis (describing), inferential analysis (inferring) and predictive analysis (predicting), as illustrated in Figure 8-2.

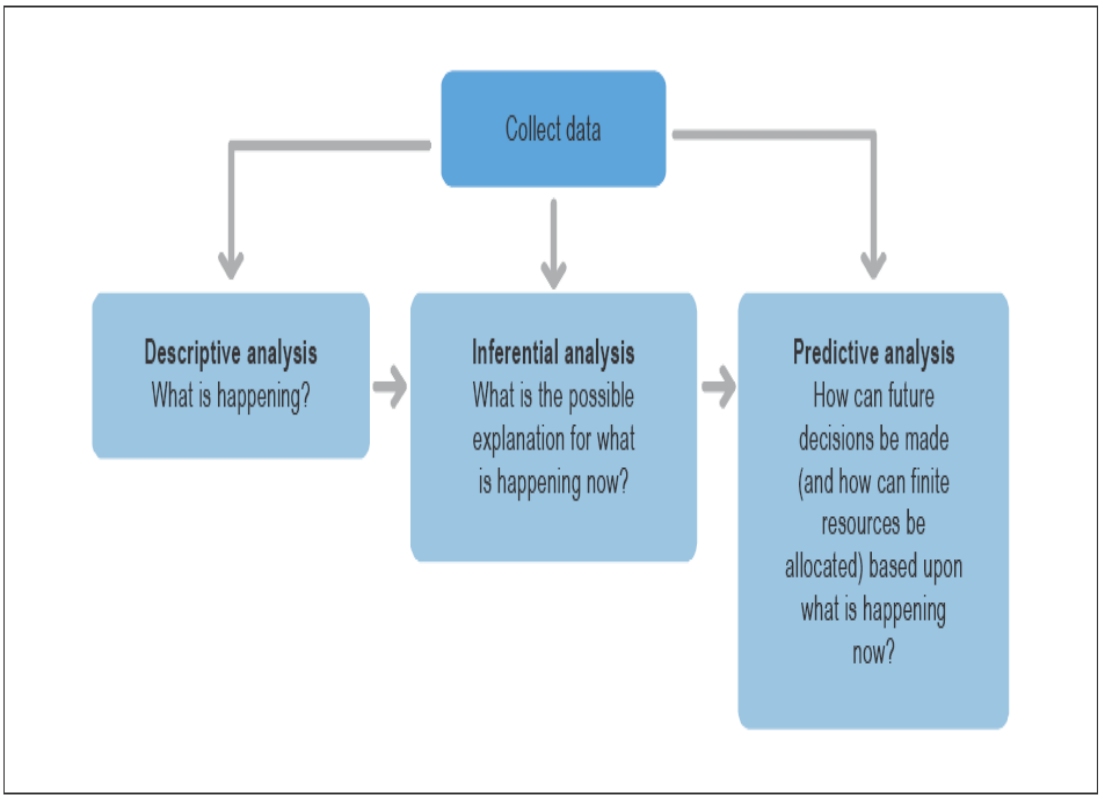

Figure 8-2: Common statistical analysis types

a) **Descriptive analysis**

Descriptive statistics are used to describe or summarize data in ways that are meaningful and useful. They help describe, show or

summarize data in ways so patterns can emerge from the data and help to clearly define case studies, opportunities and challenges. Descriptive techniques provide information about the data; however, they do not allow users to make conclusions beyond the analysed data or to reach conclusions regarding any hypotheses about the data. They are a way to describe the data.

Descriptive statistics are helpful because if we simply presented the raw data, particularly in large quantities, it would be hard to visualize what the data is showing us. Descriptive statistics enable users to present and see the data in a more meaningful way, allowing simpler interpretation of the data. Tools such as tables and matrices, graphs and charts and even maps are examples of tools used for summarizing data. Descriptive statistics include measures of central tendency such as mean (average), median and mode, as well as measures of variability such as range, quartiles, minimum and maximum, frequency distributions, variance and standard deviation (SD). These summaries may either be the initial basis for describing the data as part of a more extensive statistical analysis or they may be sufficient in and of themselves for a particular investigation.

b) **Inferential analysis**

Inferential (or inductive) statistics aim to use the data to learn about the larger population the sample of data represents. It is not always convenient or possible to examine each item of an entire population and to have access to a whole population. Inferential statistics are techniques that allow users of available data to make generalizations, inferences and conclusions about the population from which the samples were taken to describe trends. These include methods for estimating parameters, testing of statistical hypotheses, comparing the average performance of two groups on the same measure to identify differences or similarities, and identifying possible correlations and relationships among variables.

c) **Predictive analysis**

Other types of analyses include probability or predictive analyses that extract information from historical and current data and use it to predict trends and behaviour patterns. The patterns found in the data help identify emerging risks and opportunities. Often the unknown event of interest is in the future, but predictive analysis can be applied to any type of unknown in the past, present or future. The core of predictive analysis relies on capturing

relationships between variables from past occurrences and exploiting them to predict the unknown outcome. Some systems allow users to model different scenarios of risks or opportunities with different outcomes. This enables decision makers to assess the decisions they can make in the face of different unknown circumstances and to evaluate how they can effectively allocate limited resources to areas where the highest risks or best opportunities exist.

d) **Combined analysis**
Various types of statistical analyses are interconnected and often conducted together. For example, an inferential technique may be the main tool used to draw conclusions regarding a set of data, but descriptive statistics are also usually used and presented. Also, outputs of inferential statistics are often used as the basis for predictive analysis.

2) Human Resources requirements

Service providers should consider the skills necessary to analyse safety information and decide whether this role, with appropriate training, should be an extension of an existing position or whether it would be more efficient to establish a new position, outsource the role, or use a hybrid of these approaches. The decision will be driven by the plans and circumstances of each State or service provider.

3) Software requirements

In parallel with the human resourcing considerations should be an analysis of the existing software, and business and decision-making policies and processes. The safety analysis shall be integrated with the service provider's existing core tools, policies and processes. Safety data and safety information analysis can be conducted in many ways, some requiring more robust data and analytic capabilities than others. The use of suitable tools for analysis of safety data and safety information provides a more accurate understanding of the overall situation by examining the data in ways that reveal the existing relationships, connections, patterns and trends that exist within.

4) Use of analytical techniques

Analytical techniques can be applied to safety analysis in order to:

a) identify the causes and contributing factors related to hazards and elements which are detrimental to the continuous improvement of aviation safety;
b) examine areas for improvement and increase in the effectiveness
c) of safety controls; and

d) support ongoing monitoring of safety performance and trends.

5) Mature analysis capability

An organization with a mature analysis capability is better able to:

a) establish effective safety metrics;
b) establish safety presentation capabilities (e.g. safety dashboard) for ready interpretation of safety information by decision makers;
c) monitor safety performance of a given sector, organization, system or process;
d) highlight safety trends, safety targets;
e) alert safety decision makers, based on safety triggers;
f) identify factors that cause change;
g) identify connections or “correlations” between or among various factors;
h) test assumptions; and
i) develop predictive modelling capabilities.

8.9. Reporting of Analysis Results

Results of safety data analysis can highlight areas of high safety risk and assist decision makers and managers to:

a) 9

The results of a safety analysis should be made available to the service provider’s personnel and stakeholders in a way that can be easily understood. The results should be presented with the audience, such as organizational decision makers, external service providersin mind. Safety analysis results may be presented several ways; the following are some examples:

a) Imminent safety alerts: for the transmittal to other service providers of safety hazards with potential outcomes that could be catastrophic, and which require immediate actions.
b) Safety analysis reports: usually present quantitative and qualitative information with a clear description of the degree and source of the uncertainty involved in the analysis findings. These reports may also include relevant safety recommendations.
c) Safety conferences: for service providers to share safety information and safety analysis results that can promote collaborative initiatives.

It is helpful to translate recommendations into action plans, decisions and priorities that decision makers inthe organization must consider and, if possible, to outline who needs to do what about the analysis results and by when.

Visualization tools such as charts, graphs, images and dashboards are simple yet effective means of presenting results of data analysis.

8.10. Safety dashboards

The service provider shall establish a “safety dashboard”, which is a visual representation that enables senior executives, managers, and safety professionals a quick and easy way to view the organization’s safety performance.

In addition to a real time display of the organization’s SPIs and SPTs, dashboards may also include information relating to category, cause and severity of specific hazards. The information presented on the dashboard can be customized to display the information required to support the decision-making at varying levels of the organization. The use of triggers is useful for providing basic visuals to highlight if there are any issues to be addressed for a specific indicator. Analysts and decision makers will want the ability to configure the dashboard to display their top indicators as well as a feature which allows them to delve deeper into the metrics.

8.11. Safety information sharing and exchange

Sharing of safety information refers to giving, while exchange refers to giving and receiving in return.

Services providers are required to share safety information with the Authority and encouraged to exchange information across the industry.

-END-

DOC No: SCAP 007-002

Sudan Civil Aviation Authority
Sudan Safety Management Manual
February 2019