1. PURPOSE

This Advisory Circular (AC) provides guidance to service providers on safety risk assessment and mitigation.

2. REFERENCES

Civil Aviation (SMS) Regulations
Other related Tanzania Civil Aviation Regulations
ICAO Safety Management Manual (Doc 9859)
ICAO Annexes 1, 6, 8, 11, 13 and 14

3. GUIDANCE INFORMATION

3.1 Regulation 19 of the Civil Aviation (SMS) Regulations requires that a service provider shall develop and maintain a formal process that ensures analysis, assessment and control of the safety risks of the consequences of hazards during the provision of its services. It requires that the safety risks of each hazard identified through the hazard identification processes shall be analysed in terms of probability and severity of occurrence, and assessed for their tolerability. Further the regulation requires that safety risk assessment and mitigation procedures shall be developed in accordance with requirements prescribed by the Authority.

3.2 Safety risk is defined as the assessment, expressed in terms of predicted probability and severity, of the consequences of a hazard, taking as reference the worst foreseeable situation. Typically, safety risks are designated through an alphanumeric convention that allows for their measurement. Using the example of crosswind the definition of safety risk allows one to link safety risks with hazards and consequences:

a) a wind of 15 knots blowing directly across the runway is a hazard;

b) the potential for a runway lateral excursion because a pilot might not be able to control the aircraft during take-off or landing is one of the consequences of the hazard; and

c) the assessment of the consequences of a runway lateral excursion, expressed in terms of probability and severity as an alphanumerical convention, is the safety risk.

4. SAFETY RISK MANAGEMENT

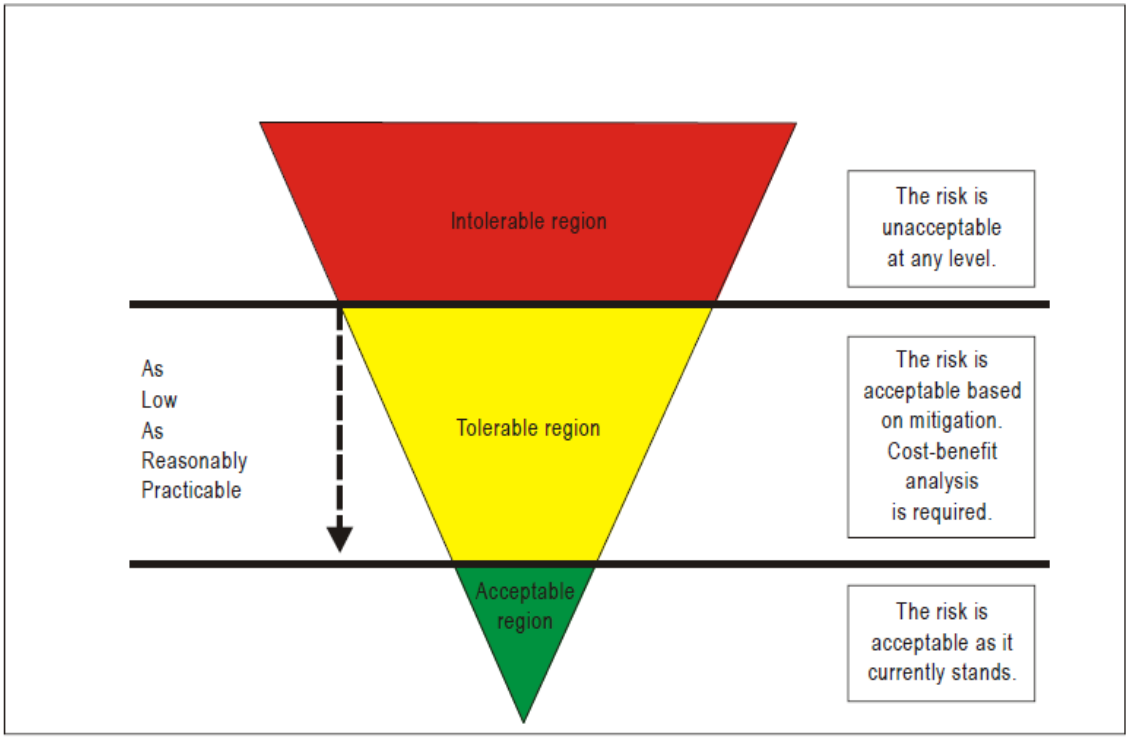
4.1 Safety risk management is a generic term that encompasses the assessment and mitigation of the safety risks of the consequences of hazards that threaten the capabilities of an organization, to a level as low as reasonably practicable (ALARP). The objective of safety risk management is to provide the foundation for a balanced allocation of resources between all assessed safety risks and those safety risks the control and mitigation of which are viable. Safety risk management is therefore a key component of the safety management process. Its added value, however, lies in the fact that it is a datadriven approach to resource allocation, thus defensible and easier to explain.

4.2 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 the viability of the organization, that immediate mitigation action is required. An organization has two alternatives to bring the safety risks to the tolerable or acceptable regions:

a) allocate resources to reduce the exposure to, and/or the magnitude of, the damaging potential of the consequences of the hazards; or

b) if mitigation is not possible, cancel the operation.

Figure 1: Safety risk management



4.3 Safety risks assessed as initially falling in the acceptable region are acceptable as they currently stand and require no action to bring or keep the probability and/or severity of the consequences of hazards under organizational control.

The same control criteria apply to safety risks initially falling in the intolerable region and mitigated to the tolerable region. A safety risk initially assessed as intolerable that is mitigated and slides down to the tolerable region must remain “protected” by mitigation strategies that guarantee its control. In both cases, a cost-benefit analysis is required:

a) Is there a return on the investment underlying the allocation of resources to bring the probability and/or severity of the consequences of hazards under organizational control? Or
b) Is the allocation of resources required of such magnitude that will pose a greater threat to the viability of the organization than bringing the probability and/or severity of the consequences of hazards under organizational control?

4.4 The acronym ALARP is used to describe a safety risk that has been reduced to a level that is as low as reasonably practicable. In determining what is "reasonably practicable" in the context of safety risk management, consideration should be given both to the technical feasibility of further reducing the safety risk, and the cost. This must include a cost-benefit analysis. Showing that the safety risk in a system is ALARP means that any further risk reduction is either impracticable or grossly outweighed by the cost. It should, however, be borne in mind that when an organization "accepts" a safety risk, this does not mean that the safety risk has been eliminated. Some residual level of safety risk remains; however, the organization has accepted that the residual safety risk is sufficiently low that it is outweighed by the benefits.

4.5 Safety risks assessed as initially falling in the acceptable region are acceptable as they currently stand and require no action to bring or keep the probability and/or severity of the consequences of hazards under organizational control.

5 SAFETY RISK ASSESSMENT

5.1 Once hazards have been identified, the safety risks of their potential consequences must be assessed. Safety risk assessment is the analysis of the safety risks of the consequences of the hazards that have been determined as threatening the capabilities of an organization. Safety risk analyses use a conventional breakdown of risk into two components the probability of occurrence of a damaging event or condition, and the severity of the event or condition, should it occur. Safety risk decision making and acceptance is specified through use of a risk tolerability matrix. While a matrix is required, discretion is also required. The definition and final construction of the matrix is left to the service provider to design, and be subject to agreement by the Authority. This is to ensure that each service provider's safety decision tools are relevant to its operations and operational environment, recognizing the extensive diversity in this area.

5.1 Safety Risk Probability

5.1.1 The process of bringing the safety risks of the consequences of hazards under organizational control starts by assessing the probability that the consequences of hazards materialize during operations aimed at delivery of services. This is known as assessing the safety risk probability.

5.1.2 Safety risk probability is defined as the likelihood that an unsafe event or condition might occur. The definition of the likelihood of a probability can be aided by questions such as:

a) Is there a history of similar occurrences to the one under consideration, or is this an isolated occurrence?
b) What other equipment or components of the same type might have similar defects?
c) How many personnel are following, or are subject to, the procedures in question?
d) What percentage of the time is the suspect equipment or the questionable procedure in use?
e) To what extent are there organizational, management or regulatory implications that might reflect larger threats to public safety?

5.1.3 Any or all of the factors underlying these example questions may be valid, underlining the importance of considering multi-causality. In assessing the likelihood of the probability that an unsafe event or condition might occur, all potentially valid perspectives must be evaluated.

5.1.4 In assessing the likelihood of the probability that an unsafe event or condition might occur, reference to historical data contained in the “safety library” of the organization is paramount in order to make informed decisions. It follows that an organization which does not have a “safety library” can only make probability assessments based, at best, on industry trends and, at worst, on opinion.

5.1.5 Based on the considerations emerging from the replies to questions such as those listed in 5.1.2, the probability that an unsafe event or condition might occur can be established and its significance assessed using a safety risk probability table. Figure 2 presents a typical safety risk probability table. The table includes five categories to denote the probability of occurrence of an unsafe event or condition, the meaning of each category, and an assignment of a value to each category.

Figure 2: Safety risk probability table

	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**

5.2 Safety Risk Severity

5.2.1 Once the safety risk of an unsafe event or condition has been assessed in terms of probability, the second step in the process of bringing the safety risks of the consequences of hazards under organizational control is the assessment of the severity of the consequences of the hazard if its damaging potential materializes during operations aimed at delivery of services. This is known as assessing the safety risk severity.

5.2.2 Safety risk severity is defined as the possible consequences of an unsafe event or condition, taking as reference the worst foreseeable situation. The assessment of the severity of the consequences of the hazard if its damaging potential materializes during operations aimed at delivery of services can be assisted by questions such as:

a) How many lives may be lost (employees, passengers, bystanders and the general public)?

b) What is the likely extent of property or financial damage (direct property loss to the operator, damage to aviation infrastructure, third-party collateral damage, financial and economic impact for the State)?

c) What is the likelihood of environmental impact (spillage of fuel or other hazardous product, and physical disruption of the natural habitat)?

d) What are the likely political implications and/or media interest?

5.2.3 Based on the considerations emerging from the replies to questions such as those listed in 5.2.2 above, the severity of the possible consequences of an unsafe event or condition, taking as reference the worst foreseeable situation, can be assessed using a safety risk severity table. Figure 3 presents a typical safety risk severity table. It includes five categories to denote the level of severity of the occurrence of an unsafe event or condition, the meaning of each category, and the assignment of a value to each category.

Figure 3: Safety risk severity table

Severity of occurrence	Meaning	Value
Catastrophic	— Equipment destroyed — Multiple deaths	**A**
Hazardous	— A large reduction in safety margins, physical distress or a workload such that the operators 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 the operators to cope with adverse operating conditions as a result of 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	— Little consequences	**E**

5.3 Safety Risk tolerability

5.3.1 Once the safety risk of the consequences of an unsafe event or condition has been assessed in terms of probability and severity, the third step in the process of bringing the safety risks of the consequences of the unsafe event or condition under organizational control is the assessment of the tolerability of the consequences of the

hazard if its damaging potential materializes during operations aimed at delivery of services. This is known as assessing safety risk tolerability. This is a two-step process.

5.3.2 First, it is necessary to obtain an overall assessment of the safety risk. This is achieved by combining the safety risk probability and safety risk severity tables into a safety risk assessment matrix, an example of which is presented in Figure 4. For example, a safety risk probability has been assessed as occasional (4). The safety risk severity has been assessed as hazardous (B). The composite of probability and severity (4B) is the safety risk of the consequences of the hazard under consideration. It can be seen, through this example, that a safety risk is just a number or alphanumerical combination and not a visible or tangible component of the natural world. The colour coding in the matrix in Figure 4 reflects the tolerability regions in the inverted triangle in Figure 1.

Figure 4: Safety risk assessment matrix

Risk probability	Risk severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

(Colour Codes for 3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E = Green to denote "Acceptable" – see figure 5)

5.3.3 Second, the safety risk index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix that describes the tolerability criteria. The criterion for a safety risk assessed as 4B is, according to the tolerability table in Figure 5, "unacceptable under the existing circumstances". In this case, the safety risk falls in the intolerable region of the inverted triangle. The safety risk of the consequences of the hazard is unacceptable. The organization must:

a) allocate resources to reduce the exposure to the consequences of the hazards;
b) allocate resources to reduce the magnitude or the damaging potential of the consequences of the hazards; or
c) cancel the operation if mitigation is not possible.

Figure 5: Safety risk tolerability matrix

Suggested criteria	Assessment risk index	Suggested criteria
Intolerable region	**5A, 5B, 5C, 4A, 4B, 3A**	Unacceptable under the existing circumstances
Tolerable region	**5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C**	Acceptable based on risk mitigation. It may require management decision.
Acceptable region	**3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E**	Acceptable

6 SAFETY RISK MITIGATION

6.1 After safety risks have been assessed though the preceding step, elimination and/or mitigation to ALARP must take place. This is known as safety risk mitigation. Safety risk controls/mitigations must be designed and implemented. These are measures to address the hazard and bring under control, the safety risk probability and severity of the consequences. These may be additional or changed procedures, new supervisory controls, changes to training, additional or modified equipment, or any of a number of other elimination/mitigation alternatives. Almost invariably these alternatives will involve deployment or re-deployment of any of the three traditional aviation defences (technology, training and regulations), or combinations of them. After the safety risk controls have been designed, but before the system is placed “online,” an assessment must be made of whether the controls introduce new hazards to the system.

6.2 There are three generic strategies for safety risk control/mitigation:

6.2.1 Avoidance. The operation or activity is cancelled because safety risks exceed the benefits of continuing the operation or activity. Examples of avoidance strategies include:

a. operations into an aerodrome surrounded by complex geography and without the necessary aids are cancelled;
b. operations in RVSM airspace by non-RVSM equipped aircraft are cancelled.

6.2.2 Reduction. The frequency of the operation or activity is reduced, or action is taken to reduce the magnitude of the consequences of the accepted risks. Examples of reduction strategies include:

a. operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to daytime, visual conditions;
b. operations by non-RVSM equipped aircraft are conducted above or below RVSM airspace.

6.2.3 Segregation of exposure. Action is taken to isolate the effects of the consequences of the hazard or build in redundancy to protect against them. Examples of strategies based on segregation of exposure include:

a. operations into an aerodrome surrounded by complex geography and without the necessary aids are limited to aircraft with specific performance navigation capabilities;
b. non-RVSM equipped aircraft are not allowed to operate into RVSM airspace.

6.3 Safety risk control/mitigation strategies are mostly based on the deployment of additional safety defences or the reinforcement of existing ones. Defences in the aviation system can be grouped under three general categories:

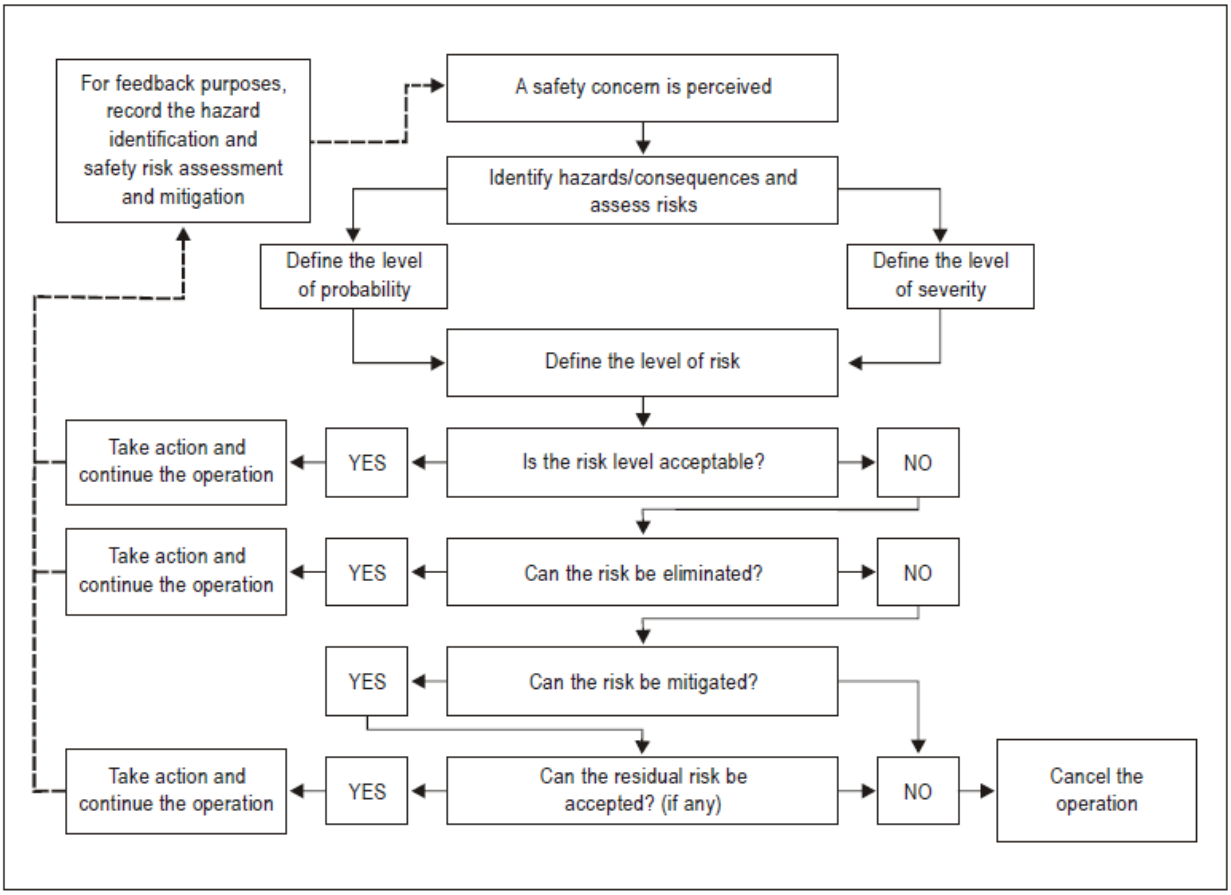
a) technology;
b) training; and
c) regulations.

6.4 As part of safety risk control/mitigation, it is important to determine if new defences are necessary or if existing ones must be reinforced. This is done by determining whether:

a) existing defences protect against the safety risks;
b) defences function as intended;
c) the defences are practical for use under working conditions;
d) staff are aware of safety risks of the consequences of the hazard and the defences in place; and
e) additional safety risk mitigation/control measures are required.

Figure 6 presents the safety risk management process in its entirety.

Figure 6: The Safety Risk Management Process



6.5 If the safety risks are assessed as unacceptable, the following questions become relevant:

a) ***Can the safety risk(s) be eliminated?*** If the answer is yes, then action as appropriate is taken and feedback to the safety library established. If the answer is no, the next question is:

b) ***Can the safety risk(s) be mitigated?*** If the answer is no, the operation must be cancelled. If the answer is yes, mitigation action as appropriate is taken and the next question is:

c) ***Can the residual safety risk be accepted?*** If the answer is yes, then action is taken (if necessary) and feedback to the safety library established. If the answer is no, the operation must be cancelled.

6.6 Question 6.5 c) reflects the fact that mitigation strategies can never completely mitigate safety risks. It must be accepted that a residual safety risk will always exist, and the organization must ensure that residual safety risks are also under control.

_____

DIRECTOR OF SAFETY REGULATION