

	TANZANIA CIVIL AVIATION AUTHORITY DIRECTORATE OF SAFETY REGULATIONS	Revision: 3 Advisory Circular
Document No.: TCAA/QSP/SR/AC/GEN-15	Title: Guidance on Safety Risk Assessment and Mitigation	Page 1 of 10

GUIDANCE ON SAFETY RISK ASSESSMENT AND MITIGATION

1.0 PURPOSE

This Advisory Circular (AC) provides guidance to service providers to conduct safety risk assessment and develop mitigation in compliance with regulatory requirements.

2.0 REFERENCES

- 2.1 The Civil Aviation (Safety Management) Regulations, 2018 as amended
- 2.2 ICAO Doc. 9859 – Safety Management Manual.
- 2.3 ICAO Doc. 9734 – Safety Oversight Manual.

3.0 BACKGROUND

3.1 Regulatory Requirements

The Civil Aviation (Safety Management) Regulations require service providers to develop and maintain a formal process that ensures analysis, assessment and control of the safety risks during the provision of its services. The safety risks of each identified hazard shall be analysed in terms of probability and severity, and assessed for their tolerability. The service provider should define safety controls for each safety risk assessed as tolerable.

3.2 Safety Risk Management

Safety Risk Management (SRM) is a key component of safety management and includes hazard identification, safety risk assessment, safety risk mitigation and risk acceptance. The term “safety risk management” is meant to differentiate this function from the management of financial risk, legal risk, economic risk and so forth. The fundamentals of safety risk management includes the following;

- a) a definition of safety risk;
- b) safety risk probability;
- c) safety risk severity;
- d) safety risk tolerability; and
- e) safety risk control/mitigation

3.3 Definition of Safety Risk

Safety risk is the projected likelihood and severity of the consequence or outcome from an existing hazard or situation. While the outcome may be an accident, an intermediate unsafe event or consequence may be identified as the most credible outcome. Provision for identification of such layered consequences is usually associated with more sophisticated risk mitigation software. The safety risk mitigation worksheet illustrated in Appendix 2 to this Advisory Circular also has this provision.

3.4 Safety Risk Probability

The process of controlling safety risks starts by assessing the probability that the consequences of hazards will materialize during aviation activities performed by the organization. Safety risk probability is defined as the likelihood that a safety consequence or outcome might occur. The determination of likelihood can be aided by questions such as:

This is a controlled document	Issued on: 29 August 2025
-------------------------------	---------------------------

- 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 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, managerial or regulatory implications that might reflect larger threats to public safety?

Any factors underlying these questions will help in assessing the likelihood that a hazard may exist, taking into consideration all potentially valid scenarios. The determination of likelihood can then be used to assist in determining safety risk probability.

Table 1 below presents a typical safety risk probability table, in this case, a five-point table. The table 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.

It must be stressed that this is an example only and that the level of detail and complexity of tables and matrices should be adapted to be commensurate with the particular needs and complexities of different organizations. Also, it should be noted that organizations may include both qualitative and quantitative criteria that may include up to fifteen values.

Table 1: Safety Risk Probability Table

Risk Probability	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occassional	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

3.5 Safety Risk Severity

Once the probability assessment has been completed, the next step is to assess the safety risk severity, taking into account the potential consequences related to the hazard. Safety risk severity is defined as the extent of harm that might reasonably occur as a consequence or outcome of the identified hazard. The severity classification should consider the following;

- a) fatalities or serious injury which would occur as a result of:
 - i) being in the aircraft;

- ii) having direct contact with any part of the aircraft, including parts which have become detached from the aircraft; or
 - iii) having direct exposure to jet blast; and
- b) damage:
- i) damage or structural failure sustained by the aircraft which:
 - aa) adversely affects the structural strength, performance or flight characteristics of the aircraft;
 - bb) would normally require major repair or replacement of the affected component;
 - ii) damage sustained by ATS or aerodrome equipment which:
 - aa) adversely affects the management of aircraft separation; or
 - bb) adversely affects landing capability

The severity assessment should consider all possible consequences related to an unsafe condition or object, taking into account the worst foreseeable situation. **Table 2**, below, presents a typical safety risk severity table. It includes five categories to denote the level of severity, the description of each category, and the assignment of a value to each category. As with the safety risk probability table, this table is an example only.

Table 2: Safety Risk Severity Table

Severity	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 on the ability of the operator 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

3.6 Safety Risk Tolerability

The safety risk probability and severity assessment process can be used to derive a safety risk index. The index created above consists of an alphanumeric designator, indicating the combined results of the probability and severity assessments. The respective severity/probability combinations are presented in the safety risk assessment matrix in **Table 3**.

The third step in the process is to determine safety risk tolerability. First, it is necessary to obtain the indices in the safety risk assessment matrix. For example, consider a situation where a safety risk probability has been assessed as occasional (4), and safety risk severity has been assessed as

hazardous (B). The composite of probability and severity (4B) is the safety risk index of the consequence.

Table 3: 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 Red to denote “Intolerable”; Yellow to denote “Tolerable”; Green to denote “Acceptable”)

The index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix {Table 4 (a)} that describes the tolerability criteria for the particular organization. Using the example above, the criterion for safety risk assessed as 4B falls in the —unacceptable under the existing circumstances/category. In this case, the safety risk index of the consequence is unacceptable.

The organization must therefore:

- take measures to reduce the organization’s exposure to the particular risk, i.e. reduce the likelihood component of the risk index;
- take measures to reduce the severity of consequences related to the hazard, i.e. reduce the severity component of the risk index; or
- cancel the operation if mitigation is not possible.

Note.— The inverted pyramid in Table 4(b) reflects a constant effort to drive the risk index towards the bottom APEX of the pyramid. Table 5 provides an example of an alternate safety risk tolerability matrix.

Table 4 (a): 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

Table 4 (b)

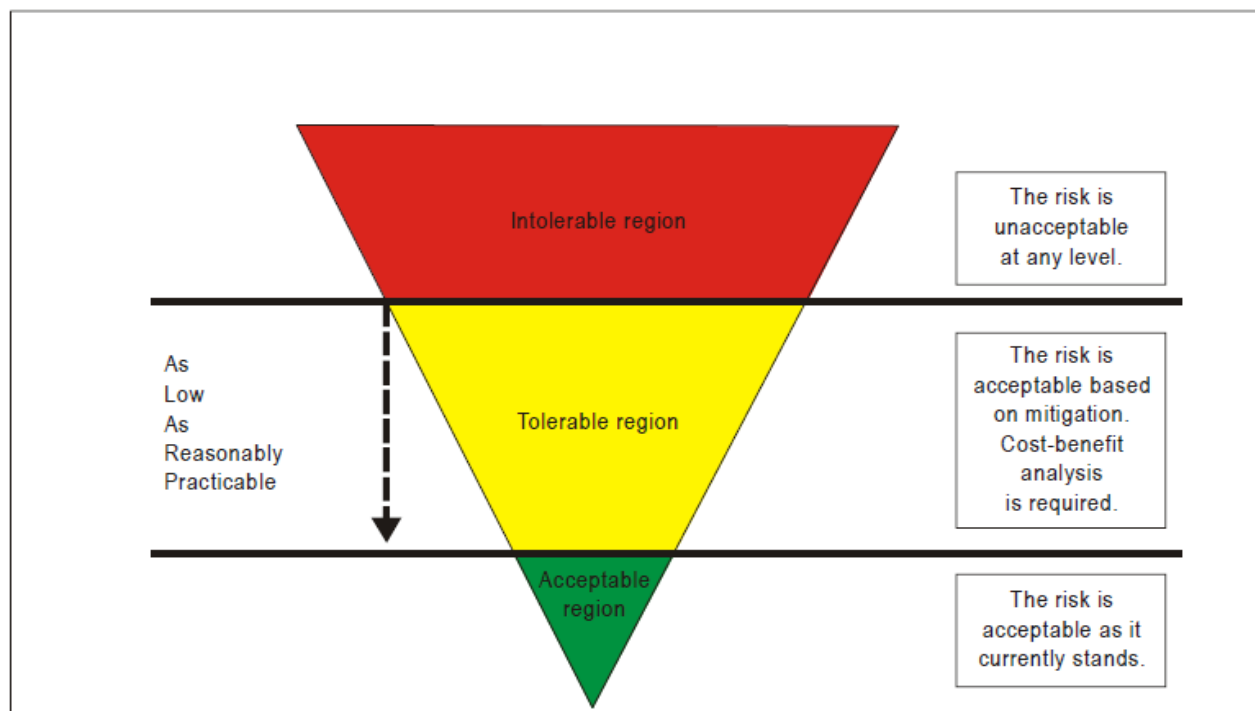


Table 5: An Alternate Safety Risk Tolerability Matrix

Risk index range	Description	Recommended action
5A, 5B, 5C, 4A, 4B, 3A	High Risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Moderate Risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable
3E, 2D, 2E, 1B, 1C, 1D, 1E	Low Risk	Acceptable as is. No further risk mitigation required

4.0 SAFETY RISK MANAGEMENT

4.1 General Principles

Safety risk management encompasses the assessment and mitigation of safety risks. The objective of safety risk management is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations. Safety risk management is therefore a key component of the safety management process at both the State and product/service provider level.

Safety risks are conceptually assessed as acceptable, tolerable or intolerable. 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, that immediate mitigation action is required.

Safety risks assessed in the tolerable region are acceptable provided that appropriate mitigation strategies are implemented by the organization. A safety risk initially assessed as intolerable may be mitigated and subsequently moved into the tolerable region provided that such risks remain controlled by appropriate mitigation strategies. In both cases, a supplementary cost-benefit analysis may be performed if deemed appropriate.

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.

4.2 Human Factors and Risk Management

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

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

4.2.2 It is therefore important to involve people with appropriate human factors expertise in the identification, assessment and mitigation of risks.

4.2.3 SRM requires all aspects of safety risk to be addressed, including those related to humans. Assessing the risks associated with human performance is more complex than risk factors associated with technology and environment since:

- human performance is highly variable, with a wide range of interacting influences internal and external to the individual. Many of the effects of the interaction between these influences are difficult, or impossible to predict; and

Document No.: TCAA/QSP/SR/AC/GEN-15	Title: Guidance on Safety Risk Assessment and Mitigation	Page 7 of 10
--	---	--------------

- b) the consequences of variable human performance will differ according to the task being performed and the context.

4.2.4 This complicates how the probability and the severity of the risk is determined. Therefore, human factors expertise is valuable in the identification and assessment of safety risks

4.3 Cost-Benefit Analysis

Cost-benefit or cost-effectiveness analysis is normally an independent process from safety risk mitigation or assessment. It is commonly associated with a higher level management protocol, such as a regulatory impact assessment or business expansion project. However, there may be situations where a risk assessment may be at a sufficiently high level or have a significant financial impact. In such situations, a supplementary CBA or cost-effectiveness process to support the risk assessment may be warranted. This is to ensure that the cost-effectiveness analysis or justification of recommended mitigation actions or preventive controls has taken into consideration the associated financial implications.

5.0 SAFETY RISK MITIGATION

5.1 General Principles

After safety risks have been assessed through the preceding step, elimination and/or mitigation to As Low As Reasonably Practicable (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.

5.2 Mitigation Strategies

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

a) **Avoidance.**

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

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

b) **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;

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

c) **Segregation of Exposure.**

This is a controlled document	Issued on: 29 August 2025
-------------------------------	---------------------------

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:

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

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.

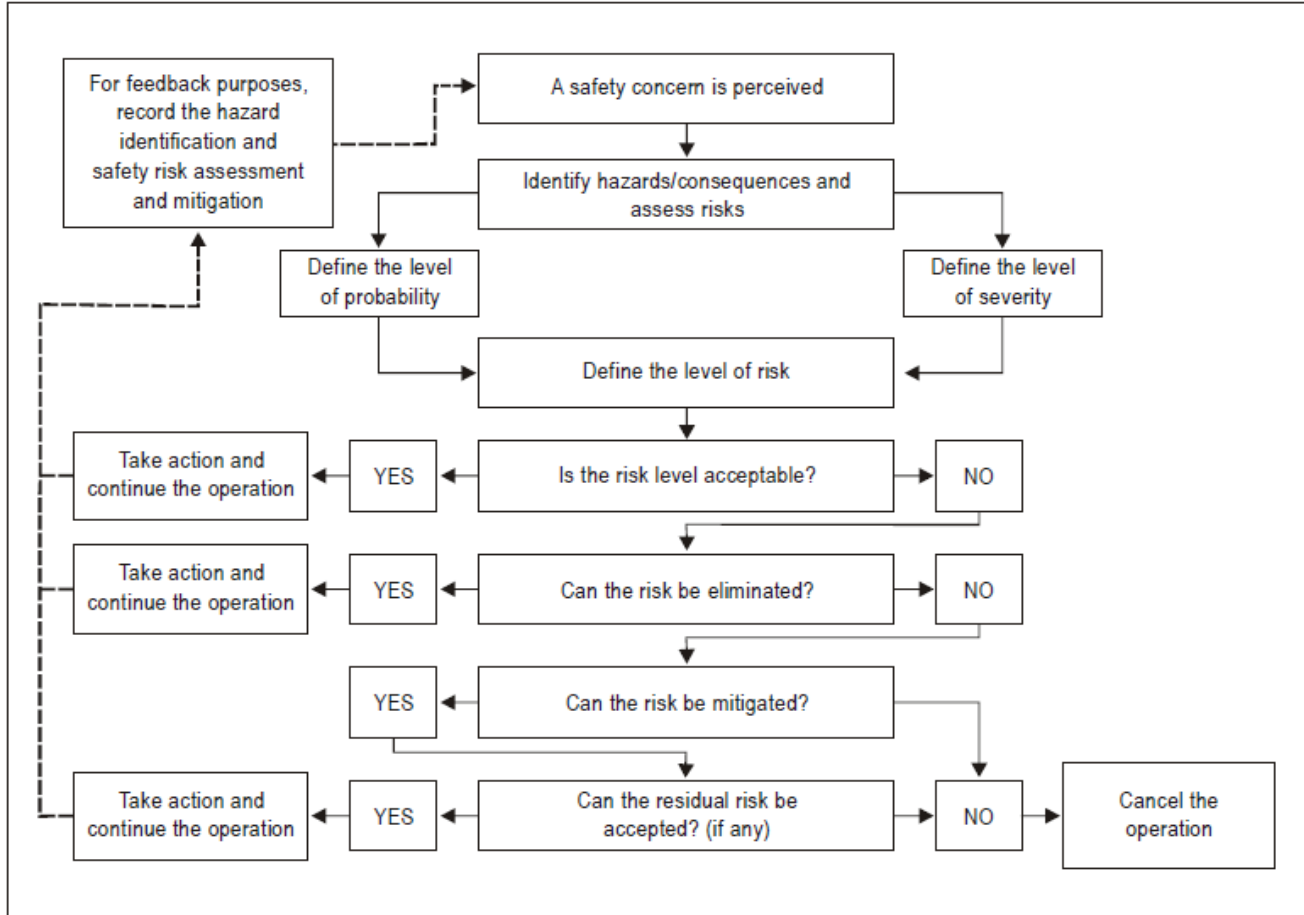
As part of safety risk control/mitigation, it is important to determine if new defences are necessary or if existing ones must be reinforced. This is done by determining whether;

- 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;
- e) additional safety risk mitigation and control measures are required.



Tanzania Civil Aviation Authority

APPENDIX 1: SAFETY RISK MANAGEMENT PROCESS



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

- 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:
- 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:
- 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.

These questions reflect 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.

APPENDIX 2 TABLE A- HAZARD AND CONSEQUENCE

Operation/process:	Describe the process/operation/equipment/system being subjected to this HIRM exercise.
Hazard (H):	If there is more than one hazard to the operation/process, use a separate worksheet to address each hazard.
Unsafe event (UE):	If there is more than one UE to the hazard, use a separate worksheet to address each UE-UC combination.
Ultimate consequence (UC):	If there is more than one UC to the hazard, use a separate worksheet to address each UC.

TABLE B - RISK INDEX AND TOLERABILITY OF CONSEQUENCE

	Current risk tolerability (taking into consideration any existing PC/RM/EC)				Resultant risk index and tolerability (taking into consideration any new PC/RM/EC)		
	Severity	Likelihood	Tolerability		Severity	Likelihood	Tolerability
Unsafe event							
Ultimate consequence							

TABLE C- RISK MITIGATION

Hazard (H)	PC	EF	EC		RM	EF	EC		
H	PC1 (Existing)	EF (Existing)	EC1 (Existing)	UE	RM1	EF (to RM1)	EC (to EF)	UC	
			EC2 (New)						
	PC2 (Existing)	EF1 (New)	EC (New)		RM2	EF (to RM2)	EC (to EF)		
		EF2 (New)	EC (New)						
	PC3 (New)	EF (New)	EC (New)		RM3	EF (to RM3)	EC (to EF)		