Public Authority for Civil Aviation

MANUAL

ON

SAFETY RISK ASSESSMENT / AERONAUTICAL STUDY

Manual Number: 1.2.7
Issue Date: 12 June 2018
Revision Number: 01

Controlled Copy

List of Effective Pages

Page No.	Rev No.	Date of Issue
1	01	12/06/18
2	01	12/06/18
3	01	12/06/18
4	01	12/06/18
5	01	12/06/18
6	01	12/06/18
7	01	12/06/18
8	01	12/06/18
9	01	12/06/18
10	01	12/06/18
11	01	12/06/18
12	01	12/06/18
13	01	12/06/18
14	01	12/06/18
15	01	12/06/18
16	01	12/06/18
17	01	12/06/18
18	01	12/06/18
19	01	12/06/18
20	01	12/06/18
21	01	12/06/18
22	01	12/06/18
23	01	12/06/18
24	01	12/06/18
25	01	12/06/18
26	01	12/06/18
27	01	12/06/18
28	01	12/06/18
29	01	12/06/18
30	01	12/06/18
31	01	12/06/18
32	01	12/06/18
33	01	12/06/18
34		
35		
36		
37		
38		
39		
40		

Page No.	Rev No.	Date of Issue
41		
42		
43		
44		
45		
46		
47		
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		
61		
62		
63		
64		
65		
66		
67		
68		
69		
70		
71		
72		
73		
74		
75		
76		
77		
78		
79		
80		

Page No.	Rev No.	Date of Issue
81		
82		
83		
84		
85		
86		
87		
88		
89		
90		
91		
92		
93		
94		
95		
96		
97		
98		
99		
100		
101		
102		
103		
104		
105		
106		
107		
108		
109		
110		
111		
112		
113		
114		
115		
116		
117		
118		
119		
120		

Table of Contents

INTENTIONALLY LEFT BLANK

Foreword

Safety risk management is one of the core activities that supports the management of safety and contributes to other indirectly related organizational processes. The objective of safety risk management is to provide the foundation for a balanced allocation of resources between all assessed safety risks, those safety risks the control and mitigation of which are viable.

The aerodrome operator operating in accordance with the requirements contained in the CAR 139 and ICAO Annex 14, shall implement a Safety Management System in accordance with the requirements given in the CAR 100 and ICAO Annex 19.

Further as per the requirements of CAR 100 and ICAO Annex 19, the "Safety Risk Management" shall be included as a component in the service providers Safety Management Systems.

This manual explains how the identified risks are analyzed in terms of probability and severity of occurrences, and assessed for their tolerability.

Therefore, all service providers/operators are advised to use the risk assessment method explained in this manual when the tolerability of the identified risks in their systems are assessed.

This manual is effective from 12 June 2018.

Anwar Bin Abdullah Al Raisi
Director General of Civil Aviation Regulation

Glossary

Acronyms and abbreviations

ALoSP	Acceptable level of safety performance
ANS	Air navigation service
ATC	Air traffic control
ATM	Air traffic management
ATS	Air traffic service(s)
CNS	Communications, navigation and surveillance
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems
ERP	Emergency response plan
H	Hazard
HIRA	Hazard identification and risk assessment
HIRM	Hazard identification and risk mitigation
ICAO	International Civil Aviation Organization
OPS	Operations
PACA	Public Authority for Civil Aviation
PC	Preventive control
SMS	Safety management system(s)
SOPs	Standard operating procedures
SPI	Safety performance indicator
SRM	Safety risk management
SSP	State safety programme
UC	Ultimate consequence
UE	Unsafe event

Definitions

Acceptable level of safety performance (ALoSP). The minimum level of safety performance of civil aviation in a State, as defined in its State safety programme, or of a service provider, as defined in its safety management system, expressed in terms of safety performance targets and safety performance indicators.

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.

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

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

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 safety parameter used for monitoring and assessing safety performance.

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

State safety programme. An integrated set of regulations and activities aimed at improving safety.

1. Introduction

1.1 A certified aerodrome operator implements an SMS acceptable to PACA that, as a minimum.

(a) Identifies safety hazards;

(b) ensures that remedial action necessary to maintain safety is implemented;

(c) Provides for continuous monitoring and regular assessment of the achieved safety; and

(d) Aims to make continuous improvement to the overall safety of the aerodrome.

1.2 This document describes how a safety assessment can be undertaken as part of the aerodrome's SMS. By applying the methodology and procedures described here, the aerodrome operator can demonstrate compliance with the minimum requirements described in 1.1.

1.3 The safety assessment process addresses the impact of a safety concern, including a change or deviation, on the safety of operations at the aerodrome and takes into consideration the aerodrome's capacity and the efficiency of operations, as necessary.

2. Definition of Safety Risk

2.1 Safety risk management is a core activity that supports the management of safety and contributes to other, indirectly related organizational processes. The term safety risk management, as opposed to the more generic term risk management, is meant to convey the notion that the management of safety does not aim — directly — at the management of financial risk, legal risk, economic risk and so forth, but restricts itself primarily to the management of safety risks.

2.2 It is a common pitfall that safety management activities oftentimes do not progress beyond hazard identification and analysis or, in other cases, jump from hazard identification direct to mitigation deployment, bypassing the evaluation and prioritization of the safety risks of the consequences of hazards. After all, once sources of danger or harm are identified, and their consequences analyzed and agreed, mitigation strategies to protect against the consequences

can certainly be deployed. This view would be correct if one were to adhere to the notion of "safety as the first priority", and focus on the prevention of bad outcomes. However, under the notion of safety management, agreeing on the consequences of identified hazards and describing them in operational terms are not enough to engage in mitigation deployment. It is necessary to evaluate the seriousness of the consequences, so as to define priorities for the allocation of resources when proposing mitigation strategies.

2.3 It is essential to somehow measure the seriousness of the consequences of hazards. This is the essential contribution of safety risk management to the safety management process. By "putting a number" on the consequences of hazards, the safety management process provides the organization with a principled basis for safety risk decisions and the subsequent allocation of organizational resources to contain the damaging potential of hazards.

2.4 The first step in addressing the confusion is narrowing down the use of the generic term risk to the very specific term safety risk. Beyond this, it is essential from the outset to establish a clear definition of safety risk and to link such a definition to the concepts of hazards and consequences expressed in operational terms.

2.5 Safety risks are not tangible or visible components of any physical or natural environment; it is necessary to think about safety risks to understand or form an image of them. Hazards and consequences, on the other hand, are tangible or visible components of a physical or natural environment, and therefore intuitive in terms of understanding and visualization. The notion of a safety risk is what is known as a construct, i.e. it is an artificial convention created by humans. In simple words, while hazards and consequences are physical components of the natural world, safety risks do not really exist in the natural world. Safety risk is a product of the human mind intended to measure the seriousness of, or "put a number" on, the consequences of hazards.

2.6 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.

3. Basic considerations

3.1 A safety assessment is an element of the risk management process of an SMS that is used to assess safety concerns arising from, inter alia, deviations from provisions and applicable regulations, identified changes at an aerodrome specified in the CAR 100, or when any other safety concerns arise.

Note: Changes on an aerodrome can include changes to procedures, equipment, infrastructures, safety works, special operations, regulations, organization, etc.

3.2 When a safety concern, change or a deviation has an impact on several aerodrome stakeholders, consideration shall be given to the involvement of all stakeholders affected in the safety assessment process. In some cases, the stakeholders impacted by the change will need to conduct a separate safety assessment themselves in order to fulfil the requirements of their SMSs and coordinate with other relevant stakeholders. When a change has an impact on multiple stakeholders, a collaborative safety assessment should be conducted to ensure compatibility of the final solutions.

3.3 A safety assessment considers the impact of the safety concern on all relevant factors determined to be safety-significant. The list below provides a number of items that may need to be considered when conducting a safety assessment. The items in this list are not exhaustive and in no particular order:

(a) aerodrome layout, including runway configurations; runway length; taxiway, taxilane and apron configurations; gates; jet bridges; visual aids; and the RFF services infrastructure and capabilities;
(b) types of aircraft, and their dimensions and performance characteristics, intended to operate at the aerodrome;
(c) traffic density and distribution;
(d) aerodrome ground services;
(e) air-ground communications and time parameters for voice and data link communications;

(f) type and capabilities of surveillance systems and the availability of systems providing controller support and alert functions;
(g) flight instrument procedures and related aerodrome equipment;
(h) complex operational procedures, such as collaborative decision-making (CDM);
(i) aerodrome technical installations, such as advanced surface movement guidance and control systems (A-SMGCS) or other air navigation aids;
(j) obstacles or hazardous activities at or in the vicinity of the aerodrome;
(k) planned construction or maintenance works at or in the vicinity of the aerodrome;
(l) any local or regional hazardous meteorological conditions (such as wind shear); and
(m) Airspace complexity, ATS route structure and classification of the airspace, which may change the pattern of operations or the capacity of the same airspace.

3.4 Subsequent to the completion of the safety assessment, the aerodrome operator is responsible for implementing and periodically monitoring the effectiveness of the identified mitigation measures.

3.5 PACA reviews the safety assessment provided by the aerodrome operator and its identified mitigation measures, operational procedures and operating restrictions, as required in 3.4 & 6 and is responsible for the subsequent regulatory oversight of their application.

4. Fundamental of Safety assessment

4.1 First Fundamental — Safety Risk Management

4.1.1 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.

4.1.2 Figure 1 depicts a broadly adopted generic visual representation of the safety risk management process. The triangle is presented in an inverted position, suggesting that aviation

(just like any other socio-technical production system) is "top heavy" from a safety risk perspective: most safety risks of the consequences of hazards will be assessed as initially falling in the intolerable region. A lesser number of safety risks of the consequences of hazards will be assessed in such a way that the assessment falls straight in the tolerable region, and an even fewer number will be assessed in such a way that the assessment falls straight in the acceptable region.

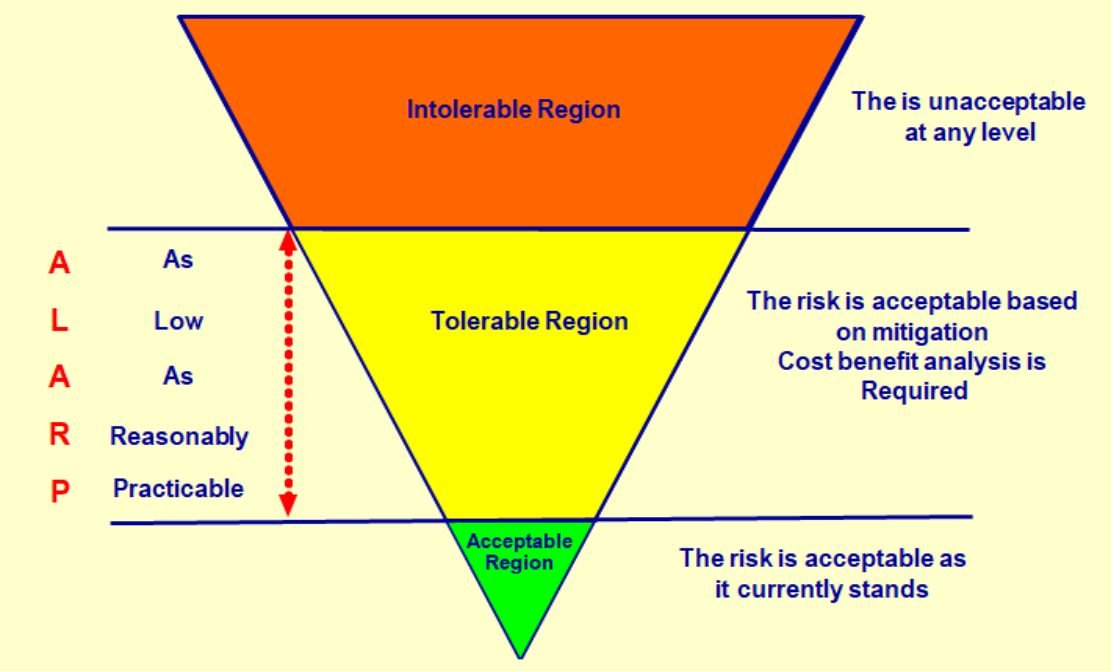


Figure 1. Safety risk management

4.1.3 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. Generally speaking, two alternatives are available to the organization 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.

4.1.4 Safety risks assessed as initially falling in the tolerable region are acceptable, provided mitigation strategies already in place guarantee that, to the foreseeable extent, the probability and/or severity of the consequences of hazards are kept 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?

4.1.5 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.

4.1.6 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.

4.1.7 Cost-benefit analyses are at the heart of safety risk management. There are two distinct costs to be considered in cost-benefit analyses: direct costs and indirect costs.

Direct costs are the obvious costs and are fairly easy to determine. They mostly relate to physical damage and include rectifying, replacing or compensating for injuries, aircraft/equipment and property damage. The high costs underlying the loss of organizational control of certain extreme consequences of hazards, such as an accident, can be reduced by insurance coverage. It must be borne in mind, however, that purchasing insurance does nothing to bring the probability and/or severity of the consequences of hazards under organizational control; it only transfers the monetary risk from the organization to the insurer. The safety risk remains unaddressed.

Indirect costs include all those costs that are not directly covered by insurance. Indirect costs may amount to more than the direct costs resulting from loss of organizational control of certain extreme consequences of hazards. Such costs are sometimes not obvious and are often delayed. Some examples of uninsured costs that may accrue from loss of organizational control of extreme consequences of hazards include:

(a) Loss of business and damage to the reputation of the organization. Many organizations will not allow their aircrafts to fly into an aerodrome with a questionable safety record.

(b) Loss of use of equipment. This equates to lost revenue. Replacement equipment may have to be purchased or leased.

(c) Loss of staff productivity. If people are injured in an occurrence and are unable to work, labour legislation may still require that they continue to receive some form of compensation. Also, these people will need to be replaced, at least for the short term, with the organization incurring the cost of wages, training, overtime, as well as imposing an increased workload on the experienced workers.

(d) Investigation and clean up. These are often uninsured costs. Operators may incur costs from the investigation including the cost of the involvement of their staff in the investigation, as well as the cost of tests and analyses, wreckage recovery and restoring the event site.

(e) Insurance deductibles. The policyholder's obligation to cover the first portion of the cost of any event must be paid. A claim will also put a company into a higher risk

category for insurance purposes and therefore may result in increased premiums. (Conversely, the implementation of safety mitigation interventions could help a company to negotiate a lower premium).

(f) Legal action and damage claims. Legal costs can accrue rapidly. While it is possible to insure for public liability and damages, it is virtually impossible to cover the cost of time lost handling legal action and damage claims.

(g) Fines and citations. Government authorities may impose fines and citations and possibly shut down unsafe operations.

Cost-benefit analyses produce results that can be numerically precise and analytically exact. Nevertheless, less exact numeric factors weigh in a cost-benefit analysis. These factors include:

(a) ***Managerial.*** Is the safety risk consistent with the organization's safety policy and objectives

(b) ***Legal.*** Is the safety risk in conformance with current regulatory standards and enforcement capabilities?

(c) ***Cultural.*** How will the organization's personnel and other stakeholders view the safety risk?

(d) ***Market.*** Will the organization's competitiveness and well-being vis-à-vis other organizations be compromised by the safety risk?

(e) ***Political.*** Will there be a political price to pay for not addressing the safety risk?

(f) ***Public.*** How influential will the media or special interest groups be in affecting public opinion regarding the safety risk?

4.2 Second Fundamental — Safety Risk Probability

4.2.1 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.

4.2.2 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?

4.2.3 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.

4.2.4 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.

4.2.5 Based on the considerations emerging from the replies to questions such as those listed in 3.2 the probability that an unsafe event or condition might occur can be established and its significance assessed using a safety risk probability table.

4.2.6 Figure 2 presents a typical safety risk probability table, in this case, a five -point 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.

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

Figure 2. Safety risk probability table

4.3 Third Fundamental — Safety Risk Severity

4.3.1 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.

4.3.2 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?

4.3.3 Based on the considerations emerging from the replies to questions such as those listed in 4.2, 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.

4.3.4 Figure 3 presents a typical safety risk severity table, also a five-point 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.

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 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

Figure 3. Safety risk severity table

4.4 Fourth Fundamental — Safety Risk Tolerability

4.4.1 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.

4.4.2 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.

4.4.3 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 4, “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.

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

Figure 4. Safety risk assessment matrix

Tolerability description	Assessed 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, 1A	Acceptable based on risk mitigation. It may require management decision.
Acceptable region	3E, 2D, 2E, 1B, 1C, 1D, 1E	Acceptable

Figure 5. Safety risk tolerability matrix

4.5 Fifth Fundamental — Safety Risk Control/Mitigation

4.5.1 In the fourth and final step of the process of bringing the safety risks of the consequences of an unsafe event or condition under organizational control, control/mitigation strategies must be deployed. Both are meant to designate measures to address the hazard and bring under organizational control the safety risk probability and severity of the consequences of the hazard.

4.5.2 Continuing with the example presented in "section 4.4" the safety risk of the consequences of the hazard under analysis has been assessed as 4B ("unacceptable under the existing circumstances"). Resources must then be allocated to slide it down the triangle, into the tolerable region, where safety risks are ALARP. If this cannot be achieved, then the operation aimed at the delivery of services which exposes the organization to the consequences of the hazards in question must be cancelled. Figure-6 presents the process of safety risk management in graphic format.

4.5.3 The 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.

(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.

(c) ***Segregation of exposure.*** Action is taken to isolate the effects of the consequences of the hazard or build in redundancy to protect against them.

4.5.4 In evaluating specific alternatives for safety risk mitigation, it must be kept in mind that not all have the same potential for reducing safety risks. The effectiveness of each specific alternative needs to be evaluated before a decision can be taken. It is important that the full range of possible control measures be considered and that trade-offs between measures be considered to find an optimal solution. Each proposed safety risk mitigation option should be examined from such perspectives as:

(a) ***Effectiveness.*** Will it reduce or eliminate the safety risks of the consequences of the unsafe event or condition? To what extent do alternatives mitigate such safety risks? Effectiveness can be viewed as being somewhere along a continuum, as follows:

(1) ***Engineering mitigations.*** This mitigation eliminates the safety risk of the consequences of the unsafe event or condition, for example, by providing interlocks to prevent thrust reverser activation in flight.

(2) ***Control mitigations.*** This mitigation accepts the safety risk of the consequences of the unsafe event or condition but adjusts the system to mitigate such safety risk by reducing it to a manageable level, for example, by imposing more restrictive operating conditions.

(3) ***Personnel mitigations.*** This mitigation accepts that engineering and/or control mitigations are neither efficient nor effective, so personnel must be taught how to cope with the safety risk of the consequences of the hazard, for example, by adding warnings, revised checklists, SOPs and/or extra training.

(b) ***Cost/benefit.*** Do the perceived benefits of the mitigation outweigh the costs? Will the potential gains be proportional to the impact of the change required?

(c) ***Practicality.*** Is the mitigation practical and appropriate in terms of available technology, financial feasibility, administrative feasibility, governing legislation and regulations, political will, etc.?

(d) ***Challenge.*** Can the mitigation withstand critical scrutiny from all stakeholders (employees, managers, stockholders/State administrations, etc.)?

(e) ***Acceptability to each stakeholder.*** How much buy-in (or resistance) from stakeholders can be expected? (Discussions with stakeholders during the safety risk assessment phase may indicate their preferred risk mitigation option.)

(f) ***Enforceability.*** If new rules (SOPs, regulations, etc.) are implemented, are they enforceable?

(g) ***Durability.*** Will the mitigation withstand the test of time? Will it be of temporary benefit or will it have long-term utility?

(h) ***Residual safety risks.*** After the mitigation has been implemented, what will be the residual safety risks relative to the original hazard? What is the ability to mitigate any residual safety risks?

(i) ***New problems.*** What new problems or new (perhaps worse) safety risks will be introduced by the proposed mitigation?

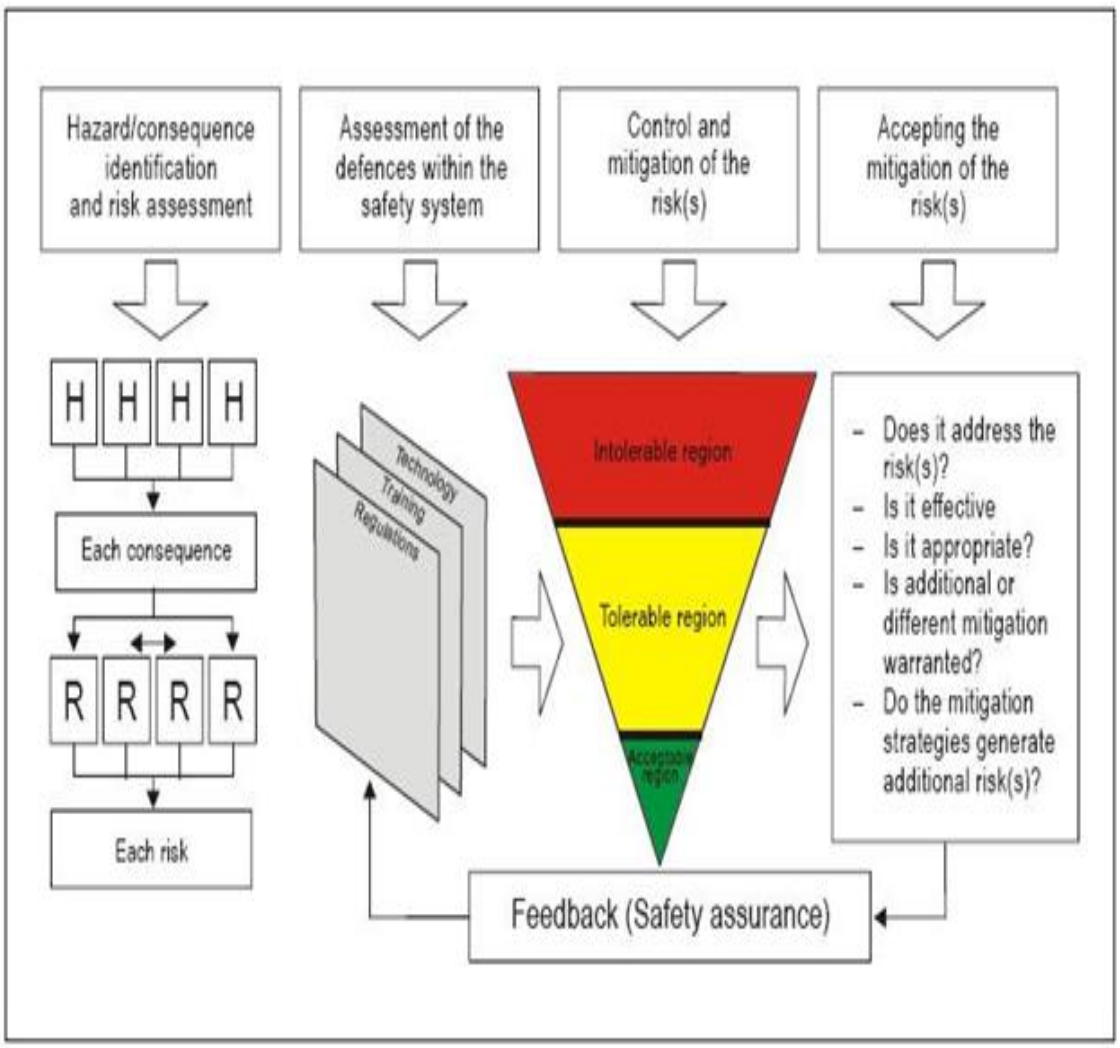


Figure 6 Global safety risk mitigation process

5. Safety Assessment Process

5.1 Introduction

5.1.1 The primary objective of a safety assessment/aeronautical study is to assess the impact of a safety concern such as a design change or deviation in operational procedures at an existing aerodrome.

5.1.2 A safety assessment/aeronautical study is conducted to assess the impact of deviations from the aerodrome provisions specified in the CAR 139 to present alternative means of ensuring

the safety of aircraft operations, to estimate the effectiveness of each alternative and to recommend procedures to compensate for the deviation.

5.1.3 A safety assessment/aeronautical study may be carried out when aerodrome standards cannot be met because of a new development or an unforeseen engineering issue, which cannot be rectified easily. Such a study is most frequently undertaken during the planning of a new airport or during the certification of an existing aerodrome.

5.1.4 Such a safety concern can often impact multiple stakeholders; therefore, safety assessments often need to be carried out in a cross-organizational manner, involving experts from all the involved stakeholders. Prior to them assessment, a preliminary identification of the required tasks and the organizations to be involved in the process is conducted.

5.1.5 A safety assessment is initially composed of four basic steps explained below:

(a) Definition of a safety concern and identification of the regulatory compliance;
(b) Hazard identification and analysis;
(c) Risk assessment and development of mitigation measures; and
(d) Development of an implementation plan for the mitigation measures and conclusion of the assessment.

5.1.6 A safety assessment process flow chart applicable for aerodrome operations is provided in the Figure-7.

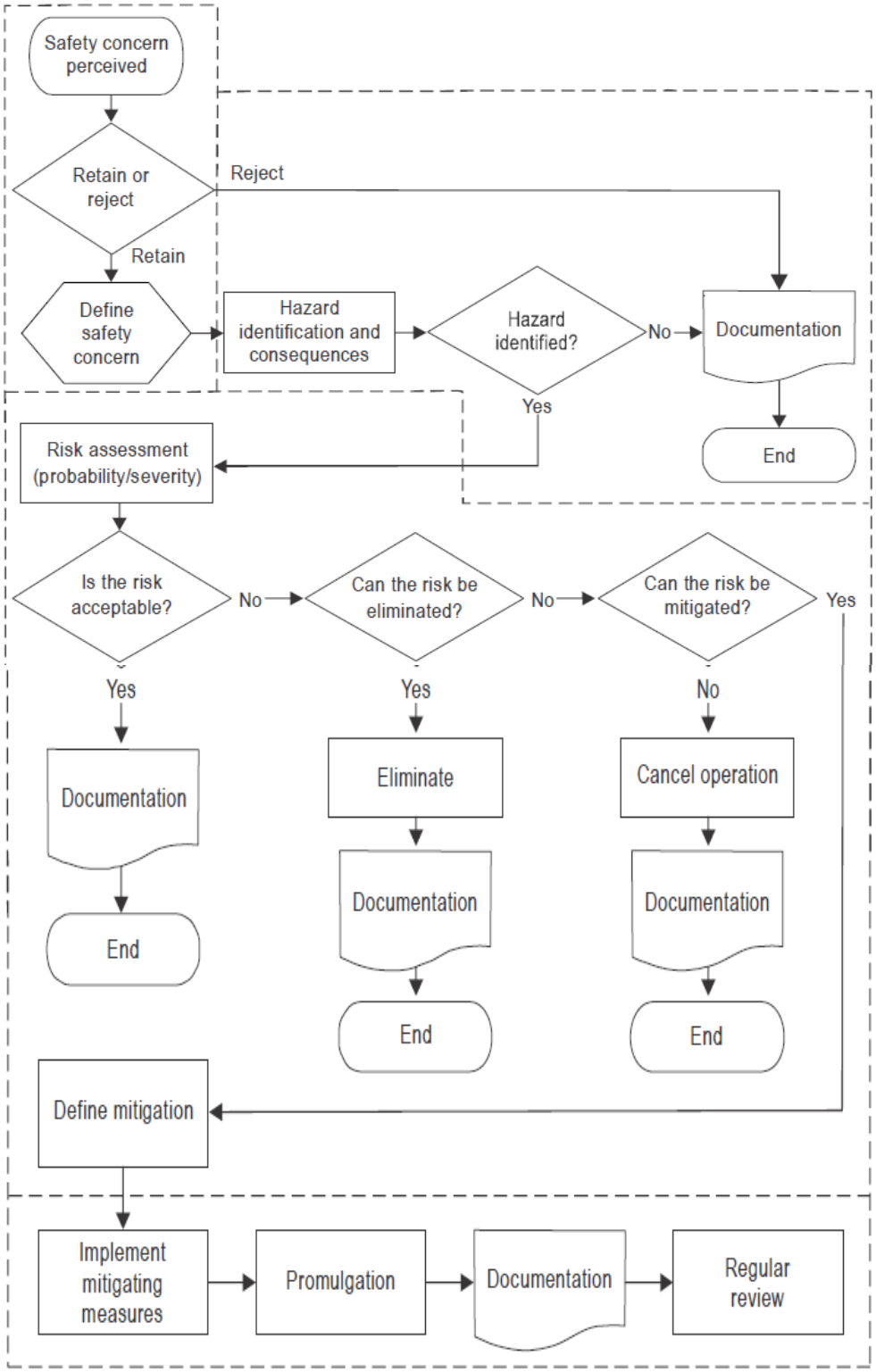


Figure 7 –Flow chart to be used for the conduct of a safety assessment

5.2 Definition of a safety concern and identification of the regulatory compliance

5.2.1 Any perceived safety concerns are to be described in detail, including timescales, projected phases, location, stakeholders involved or affected as well as their potential influence on specific processes, procedures, systems and operations.

5.2.2 The perceived safety concern is first analysed to determine whether it is retained or rejected. If rejected, the justification for rejecting the safety concern is to be provided and documented.

5.2.3 An initial evaluation of compliance with the appropriate provisions in the regulations applicable to the aerodrome is conducted and documented.

5.2.4 The corresponding areas of concern are identified before proceeding with the remaining steps of the safety assessment, with all relevant stakeholders.

Note.— It may be useful to review the historical background of some regulatory provisions to gain a better understanding of the safety objective of those provisions.

5.2.5 If a safety assessment was conducted previously for similar cases in the same context at an aerodrome where similar characteristics and procedures exist, the aerodrome operator may use some elements from that assessment as a basis for the assessment to be conducted. Nevertheless, as each assessment is specific to a particular safety concern at a given aerodrome the suitability for reusing specific elements of an existing assessment is to be carefully evaluated.

5.3 Hazard identification

5.3.1 Hazards related to infrastructure, systems or operational procedures are initially identified using methods such as brain-storming sessions, expert opinions, industry knowledge, experience and operational judgement. The identification of hazards is conducted by considering:

(a) accident causal factors and critical events based on a simple causal analysis of available accident and incident databases;
(b) events that may have occurred in similar circumstances or that are subsequent to the resolution of a similar safety concern; and

(c) potential new hazards that may emerge during or after implementation of the planned changes.

5.3.2 Following the previous steps, all potential outcomes or consequences for each identified hazard are identified.

Note.1— Further guidance on the definition of risk can be found in Doc 9859.

Note.2— Appendix 1 - Example of a Safety Risk Mitigation Worksheet

5.3.3 The appropriate safety objective for each type of hazard should be defined and detailed. This can be done through:

(a) reference to recognized standards and/or codes of practices;

(b) reference to the safety performance of the existing system;

(c) reference to the acceptance of a similar system elsewhere; and

(d) application of explicit safety risk levels.

5.3.4 Safety objectives are specified in either quantitative terms (e.g. identification of a numerical probability) or qualitative terms (e.g. comparison with an existing situation). The selection of the safety objective is made according to the aerodrome operator's policy with respect to safety improvement and is justified for the specific hazard.

5.4 Risk assessment and development of mitigation measures

5.4.1 The level of risk of each identified potential consequence is estimated by conducting a risk assessment. This risk assessment will determine the severity of a consequence (effect on the safety of the considered operations) and the probability of the consequence occurring and will be based on experience as well as on any available data (e.g. accident database, occurrence reports).

5.4.2 Understanding the risks is the basis for the development of mitigation measures, operational procedures and operating restrictions that might be needed to ensure safe aerodrome operations.

5.4.3 The method for risk evaluation is strongly dependent on the nature of the hazards. The risk itself is evaluated by combining the two values for severity of its consequences and probability of occurrence.

Note.— see Attachment to Appendix 1. Example Severity, Likelihood, Risk Index and Tolerability Tables

5.4.4 Once each hazard has been identified and analysed in terms of causes, and assessed for severity and probability of its occurrence, it must be ascertained that all associated risks are appropriately managed. An initial identification of existing mitigation measures must be conducted prior to the development of any additional measures.

5.4.5 All risk mitigation measures, whether currently being applied or still under development, are evaluated for the effectiveness of their risk management capabilities.

Note.— The exposure to a given risk (e.g. duration of a change, time before implementation of corrective actions, traffic density) is taken into account in order to decide on its acceptability.

5.4.6 In some cases, a quantitative approach may be possible, and numerical safety objectives can be used. In other instances such as changes to the operational environment or procedures, a qualitative analysis may be more relevant.

Note 1.— An example of a qualitative approach is the objective of providing at least the same protection as the one offered by the infrastructure corresponding to the appropriate reference code for a specific aeroplane.

5.4.7 The Methodologies for risk management can be found in paragraph 4 of this document.

5.4.8 In some cases, the result of the risk assessment may be that the safety objectives will be met without any additional specific mitigation measures.

5.5 Development of an implementation plan and conclusion of the assessment

5.5.1 The last phase of the safety assessment process is the development of a plan for the implementation of the identified mitigation measures.

5.5.2 The implementation plan includes time frames, responsibilities for mitigation measures as well as control measures that may be defined and implemented to monitor the effectiveness of the mitigation measures.

6. Approval or acceptance of a safety assessment

6.1 The safety assessments made by the aerodrome operator or any other party (Public) related to deviation from the CAR 139 provisions or other regulations must be approved by PACA.

6.2 The safety assessments made by the aerodrome operator related to a major change in operational procedures or in infrastructure must be sent to PACA for Information.

6.3 a safety assessment subject to approval or acceptance by PACA be submitted by the aerodrome operator prior to implementation.

6.4 PACA analyses the safety assessment and verifies that:

(a) appropriate coordination has been performed between the concerned stakeholders;
(b) the risks have been properly identified and assessed, based on documented arguments (e.g. physical or Human Factors studies, analysis of previous accidents and incidents);
(c) the proposed mitigation measures adequately address the risk; and
(d) the time frames for planned implementation are acceptable.

Note.— It is preferable to work with a team of the State's operational experts in the areas considered in the safety assessment.

6.5 On completion of the analysis of the safety assessment, PACA:

(a) either gives formal approval or acceptance of the safety assessment to the aerodrome operator as required in 3.5.1; or
(b) if some risks have been underestimated or have not been identified, coordinates with the aerodrome operator to reach an agreement on safety acceptance; or
(c) if no agreement can be reached, rejects the proposal for possible resubmission by the aerodrome operator; or
(d) may choose to impose conditional measures to ensure safety.

6.6 PACA should ensure that the mitigation or conditional measures are properly implemented and that they fulfil their purpose.

7. Promulgation of safety information

7.1 The aerodrome operator must determine the most appropriate method for communicating safety information to the stakeholders and ensures that all safety-relevant conclusions of the safety assessment are adequately communicated.

7.2 In order to ensure adequate dissemination of information to interested parties, information that affects the current integrated aeronautical information package (IAIP) or other relevant safety information is:

(a) promulgated in the relevant section of the IAIP or automatic terminal information service (ATIS); or

(b) published in the relevant aerodrome information communications through appropriate means after PACA approval.

7.3 PACA shall verify that the outcomes of risk assessments / aeronautical studies, in the form of exceptions, are published in a document, which is publicly accessible, such as the State AIP or other means of information.

8. Review the validity of using an aeronautical study or risk assessment

In order to review the validity of using an aeronautical study / risk assessment, PACA shall:

- Conduct a regular review of exemptions or exceptions granted to assess their continued validity or whether the cause can be removed.
- Conduct a review of exemptions or exceptions which are to be issued against the applicable provisions to determine if a change in the notification status of differences to provisions should be filed.

Appendix 1 - Example of a Safety Risk Mitigation Worksheet

Note.— For easier worksheet management, it is preferable to use a separate worksheet for each different Hazard>Unsafe event>Ultimate consequence combination.

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 1-A1-1. Hazard and 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 2-A1-2. Risk index and tolerability of consequence/UE (see Attachment 1)

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)	

Table 2-A2-3. Risk mitigation

Explanatory notes.—

1. *Operation/process (Table 1-A1-1).* Description of the operation or process which is being subjected to this hazard/risk mitigation exercise.

2. *Hazard (H).* An undesirable condition or situation which may lead to unsafe event(s) or occurrence(s). Sometimes the term "threat" (e.g. TEM) is used instead of "hazard".

3. *Unsafe event (UE).* A possible intermediate unsafe event before any ultimate consequence, accident or most credible outcome. Identification of an unsafe event is applicable only where there is a need to distinguish and establish mitigating actions upstream and downstream of such an intermediate event (before the ultimate consequence/accident) (e.g. "over temperature event" before an "engine failure"). If this intermediate UE state is not applicable for a particular operation, then it may be excluded as appropriate.

4. *Ultimate consequence (UC).* The most credible outcome, ultimate event or accident.

5. *Preventive control (PC).* A mitigating action/mechanism/defence to block or prevent a hazard/threat from escalating into an unsafe event or ultimate consequence.

6. *Escalation factor (EF).* A possible latent condition/factor which may weaken the effectiveness of a preventive control (or recovery measure). Use where applicable only. It is possible that an escalation factor may sometimes be referred to as a "threat".

7. *Escalation control (EC).* A mitigating action/mechanism to block or prevent an escalation factor from compromising or weakening a preventive control (or recovery measure). Use where applicable only.

8. *Current risk index and tolerability.* Risk mitigating action (Table 2-A1-3) is applicable whenever an unacceptable current tolerability level of an unsafe event or ultimate consequence is identified in Table 2-A1-2. Current risk index and tolerability shall take into consideration existing preventive controls, where available.

9. *Resultant risk index and tolerability.* Resultant risk index and tolerability are based on the combined current preventive controls (if any) together with the new preventive controls/escalation controls/recovery measures put in place as a result of the completed risk mitigation exercise.

Attachment to Appendix 1. Example Severity, Likelihood, Risk Index and Tolerability Tables

Level	Descriptor	Severity description (customise according to the nature of the product or the service provider's operations)
A	Catastrophic	Loss of aircraft
B	Major	Complete failure of significant/major aircraft systems or results in emergency application of flight operations procedures
C	Moderate	Partial loss of significant/major aircraft systems or results in abnormal application of flight operations procedures
D	Minor	Degrades or affects normal aircraft operational procedures or performance
E	Insignificant	No significance to aircraft-related operational safety

Table Att-1. Severity table (basic)

Level	Descriptor	*Severity description (customize according to the nature of the product or service provider's operations)*					
		Safety of aircraft	*Physical injury*	*Damage to assets*	*Potential revenue loss*	*Damage to environment*	*Damage to corporate reputation*
A	Catastrophic	Aircraft/hull loss	Multiple fatality	Catastrophic damage More than $__	Massive loss More µthan $__	Massive effect	International implication
B	Major	Complete failure of significant/major Aircraft systems or results in emergency application of flight operations procedures	Single fatality	Major damage Less than $__	Major loss Less than $__	Major effect	National Implication
C	Moderate	Partial loss of significant/major aircraft systems or results in abnormal flight operations procedure application	Serious injury	Substantial damage Less than $__	Substantial loss Less than $__	Contained effect	Regional Implication
D	Minor	Degrades or affects normal aircraft operational procedures or performance	Minor injury	Minor damage Less than $__	Minor loss Less Than $__	Minor effect	Limited localized implication
E	Insignificant	No significance to aircraft related operational safety	No injury	No damage	No revenue loss	No effect	No implication

Note.— Use the highest severity level obtained to derive the risk index in the risk index matrix table.

Table Att-2. Severity table (alternate)

Level	Descriptor	
1	Exceptional	May occur only in exceptional circumstances
2	Unlikely/improbable	Could occur at some time
3	Possible/remote	Might occur at some time
4	Likely/occasional	Will probably occur at some time
5	Certain/frequent	Is expected to occur in most circumstances

Table Att-3. Likelihood table

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

Table Att-4. Risk index matrix (severity × likelihood)

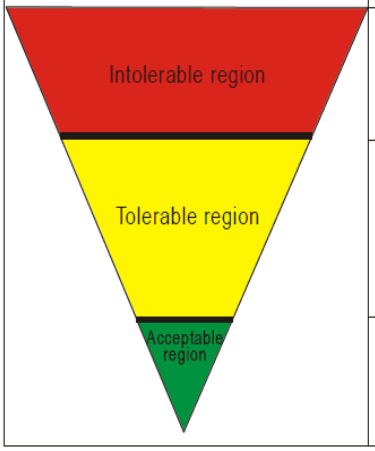
Tolerability description	Assessed risk index	Suggested criteria
	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Acceptable based on risk mitigation. It may require management decision.
	3E, 2D, 2E, 1B, 1C, 1D, 1E	Acceptable

Table Att-5. Risk acceptability (tolerability) table

-END-