Advisory Circular

CAA-AC-SMS007A

July, 2020

GUIDANCE ON SAFETY RISK MANAGEMENT PROCESSES

1.0 PURPOSE

1.1 This Advisory Circular (AC) provides guidance to service providers on Safety Risk Management, which include Hazard Identification, Safety Risk Assessment, Safety Risk Mitigation and Risk acceptance. Safety Risk Management is a component of the Safety Management Systems (SMS) framework as provided for in the Civil Aviation (Safety Management) Regulations.

1.2 Safety risk assessment should allow for consistent and systematic approach for the assessment of safety risks, this should include methods that determine what safety risks are acceptable or unacceptable and prioritize actions.

1.3 The Civil Aviation (Safety Management) Regulations require service providers to develop and maintain a formal process that ensures hazard identification. The hazard identification process shall be developed in accordance to requirements prescribed by the Authority. Further, 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 of the consequences of hazards during the provision of its services. This Advisory Circular therefore prescribes the Authority's requirements to enable service providers to comply with the provisions of the regulations.

1.4 This Advisory Circular supersedes **CAA-AC-SMS007**.

2.0 REFERENCES

2.1 The Civil Aviation Act;

2.2 The Civil Aviation (Safety Management) Regulations, as amended;

3.0 HAZARD IDENTIFICATION PROCESS

3.1 Introduction

3.1.1 A hazard is identified as a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function. Hazard identification is a core process in the management of safety. Hazards may be identified through reactive, proactive and predictive process. Reactive processes involve identification of hazard through accidents and incidents that have occurred. Proactive and predictive processes involve identification of hazards before they precipitate safety events.

3.1.2 Hazard identification is the first step in a formal process of collecting, recording, acting on and generating feedback about hazards and safety risks in operations The hazard identification process will involve reporting of hazards, events or safety concerns; collection and storage of safety data; analysis of the safety data; and distribution of the safety information distilled from the safety data.

3.2 Scope of Factors and Processes in Hazard Identification

3.2.1 The scope of factors and processes to be considered by a service provider when engaging in hazard identification should include:

3.2.1.1 Equipment design;
3.2.1.2 Procedures and operating practices;
3.2.1.3 Communication;
3.2.1.4 Personnel factors;
3.2.1.5 Organizational factors;
3.2.1.6 Work environment;
3.2.1.7 Regulatory oversight factors;
3.2.1.8 System defenses; and
3.2.1.9 Human performance.

3.3 Sources of Hazard Identification

3.3.1 There are a variety of sources of hazard identification. Some sources are internal to the organization while other sources are external to the organization.

3.3.2 Examples of the internal sources of hazard identification available to an organization include:
3.3.2.1 flight data analysis;
3.3.2.2 company voluntary reporting system;
3.3.2.3 safety surveys;
3.3.2.4 safety audits;
3.3.2.5 normal operations monitoring schemes;
3.3.2.6 trend analysis;
3.3.2.7 feedback from training; and
3.3.2.8 investigation and follow-up of incidents.

3.3.3 Examples of external sources of hazard identification available to an organization include:
3.3.3.1 Accident reports;
3.3.3.2 State mandatory occurrence reporting system;
3.3.3.3 State voluntary reporting system;
3.3.3.4 State oversight audits; and
3.3.3.5 Information exchange systems.

3.3.4 The fundamental point to note is that no source or programme entirely replaces others, or makes other sources or programmes redundant or unnecessary. Hazard identification conducted under mature safety management practices resorts to a judicious combination of internal and external sources, reactive, proactive and predictive processes, and their underlying programmes.

3.3.5 All personnel in aviation organizations should receive the appropriate safety management training, at a level commensurate with their responsibilities, so that everybody in the organization is prepared and able to identify and report hazards. From this perspective, hazard identification and reporting are everybody's responsibility. However, organizations must have designated personnel with the exclusive charge of hazard identification and analysis. This would normally be the personnel assigned to the safety services office. Therefore, broadening the previous perspective, in aviation organizations, hazard identification is everybody's responsibility, but accountability for hazard identification lies with dedicated safety personnel.

3.3.6 How hazards are identified will depend on the resources and constraints of each particular organization. Some organizations will deploy comprehensive, technology-intensive hazard identification programmes. Other organizations will deploy modest hazard identification programmes better suited to their size and the complexity of their operations. Nevertheless, hazard identification, regardless of implementation, complexity and size, must be a formal process, clearly described in the organization's safety documentation. Ad hoc hazard identification is an unacceptable safety management practice.

3.3.7 Under mature safety management practices, hazard identification is a continuous, ongoing, daily activity. It never stops or rests. It is an integral part of the organizational processes aimed at delivering the services that the organization is in business to deliver. Nevertheless, there are three

specific conditions under which special attention to hazard identification is warranted. These three conditions should trigger more in-depth and far-reaching hazard identification activities and include:

3.3.7.1 any time the organization experiences an unexplained increase in safety-related events or regulatory infractions;

3.3.7.2 any time major operational changes are foreseen, including changes to key personnel or other major equipment or systems; and

3.3.7.3 before and during periods of significant organizational change, including rapid growth or contraction, corporate mergers, acquisitions or downsizing.

3.4 Hazard Identification Process

3.4.1 The hazard identification process shall include the following steps:

3.4.1.1 Step 1: reporting of hazards, events or safety concerns;

3.4.1.2 Step 2: collection and storage of safety data;

3.4.1.3 Step 3: analysis of the safety data; and

3.4.1.4 Step 4: distribution of the safety information distilled from the safety data.

3.4.2 Hazard analysis is the first step in developing safety information is. Hazard analysis is a three-step process:

3.4.2.1 ***First step.*** Identify the generic hazard (also known as top level hazard, or TLH). Generic hazard is used as a term that intends to provide focus and perspective on a safety issue, while also helping to simplify the tracking and classification of many individual hazards flowing from the generic hazard.

3.4.2.2 ***Second step.*** Break down the generic hazard into specific hazards or components of the generic hazard. Each specific hazard will likely have a different and unique set of causal factors, thus making each specific hazard different and unique in nature.

3.4.2.3 ***Third step.*** Link specific hazards to potentially specific consequences, i.e. specific events or outcomes.

An example is provided to illustrate the notions of generic hazard, specific hazard and consequences. An international airport that handles 100,000 movements per year launches a construction project to extend and re-pave one of two crossing runways. The following three-step hazard analysis process would apply:

*a) **Step A.** State the generic hazard (hazard statement or TLH)*
— airport construction

*b) **Step B.** Identify specific hazards or components of the generic hazard*
— construction equipment
— closed taxiways, etc.

*c) **Step C.** Link specific hazards to specific consequence(s)*
— aircraft colliding with construction equipment (construction equipment)
— aircraft taking off into the wrong taxiway (closed taxiways), etc.

3.4.3 The runway construction example discussed above can be used to extend the discussion about the "dilemma of the two Ps" to hazard analysis: efficient and safe provision of service requires a constant balance between production goals and safety goals. In the case of the runway construction example, there is clearly an efficiency (production) goal: maintaining regular aerodrome operations during a runway construction project. There is an equally clear safety (protection) goal: maintaining existing margins of safety of aerodrome operations during the runway construction project. In conducting the hazard analysis, two basic premises of safety management must be at the forefront of the analyses:

3.4.3.1 hazards are potential vulnerabilities inherent in socio-technical production systems. They are a necessary part of the system as a result of the capabilities they provide or can potentially provide to the system to deliver its services. Aviation workplaces therefore contain hazards which may not be cost-effective to address even when operations must continue; and

3.4.3.2 hazard identification is a wasted effort if restricted to the aftermath of rare occurrences where there is serious injury or significant damage.

3.4.4 Safety risk management starts with a description of the system's functions as the basis for hazard identification. In the system description, the system components and their interfaces with the system's operational environment are analyzed for the presence of hazards, as well as to identify those safety risk controls already existing in the system or the absence thereof (a process known as gap analysis. Hazards are analyzed within the context of the described system, their potentially damaging consequences identified, and such consequences assessed in terms of safety risks. Where the safety risks of the consequences of hazards are assessed to be too high to be acceptable, additional safety risk controls must be built into the system. Assessment of system design and verification that it adequately controls the consequences of hazards is, therefore, a fundamental element of safety management.

3.4.5 A structured approach to the identification of hazards ensures that, as much as possible, most hazards in the system's operational environment are identified. Suitable techniques for ensuring such a structured approach might include:

3.4.5.1 ***Checklists.*** Review experience and available data from similar systems and draw up a hazard checklist. Potentially hazardous areas will require further evaluation.

3.4.5.2 ***Group review.*** Group sessions may be used to review the hazard checklist, to brainstorm hazards more broadly, or to conduct a detailed scenario analysis.

3.4.6 Hazard identification sessions require a range of experienced operational and technical personnel and are usually conducted through a form of managed group discussion. A facilitator who is familiar with brainstorming techniques should manage the group sessions. A safety manager, if appointed, would normally fill this role. While the use of group sessions is addressed here in the context of hazard identification, the same group would also address the assessment of the probability and severity of the safety risks of the consequences of the hazards they have identified.

3.4.7 The assessment of hazards should take into consideration all possibilities, from the least to the most likely. It has to make adequate allowance for "worst-case" conditions, but it is also important that the hazards to be included in the final analysis be "credible" hazards. It is often difficult to define the boundary between the worst credible case and one so dependent on coincidence that it should not be taken into account. The following definitions can be used as a guide in making such decisions:

3.4.7.1 ***Worst case.*** The most unfavourable conditions expected, e.g. extremely high levels of traffic and extreme weather disruption.

3.4.7.2 ***Credible case.*** This implies that it is not unreasonable to expect that the assumed combination of extreme conditions will occur within the operational life cycle of the system.

3.4.8 All identified hazards should be assigned a hazard number and be recorded in a hazard log. The hazard log should contain a description of each hazard, its consequences, the assessed likelihood and severity of the safety risks of the consequences, and required safety risk controls, most usually,

mitigation measures. The hazard log should be updated as new hazards are identified and proposals for further safety risk controls (i.e. further mitigation measures) are introduced.

Table 1- illustration of hazard prioritization procedure

<table>
<tr><th></th><th>Option 1 (Basic)</th><th>Option 2 (Advanced)</th></tr>
<tr><td>Criteria</td><td>Prioritize in relation to the hazard's worst possible consequence (incident severity) category.</td><td>Prioritize in relation to the risk index (severity and likelihood) category of the hazard's worst possible consequence.</td></tr>
<tr><td>Methodology</td><td>a) project the hazard's worst possible consequence;

b) project the likely occurrence classification of this consequence (i.e. will it be deemed to be an accident, serious incident or incident?);

c) conclude that the hazard's prioritization is thus:
<table><tr><th>Projected consequence</th><th>Hazard level</th></tr><tr><td>Accident
Serious incident
Incident</td><td>Level 1
Level 2
Level 3</td></tr></table></td><td>a) project the risk index number (based on the relevant severity and likelihood matrix) of the hazard's worst possible consequence (refer to Figure 2-13 of this chapter);

b) with reference to the related tolerability matrix, determine the risk index's tolerability category (i.e. intolerable, tolerable or acceptable) or equivalent terminology/ categorization;

c) conclude that the hazard's prioritization is thus:
<table><tr><th>Projected risk index</th><th>Hazard level</th></tr><tr><td>Intolerable/High risk
Tolerable/Moderate risk
Acceptable/Low risk</td><td>Level 1
Level 2
Level 3</td></tr></table></td></tr>
<tr><td>Remarks</td><td>Option 1 takes into consideration the severity of the hazard's projected consequence only.</td><td>Option 2 takes into consideration the severity and likelihood of the hazard's projected consequence — a more comprehensive criteria than Option 1.</td></tr>
</table>

Note.— From a practical viewpoint, Option 1 is more viable than Option 2 for the purpose of a simpler prioritization system. The purpose of such a system is to facilitate sorting and prioritization of hazards for risk mitigation

4.0 SAFETY RISK ASSESSMENT

4.1 Safety risk management is a key component of a safety management system. 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 includes the following:

4.1.1 a definition of safety risk;
4.1.2 safety risk probability;
4.1.3 safety risk severity;
4.1.4 safety risk tolerability; and
4.1.5 safety risk management

4.2 Definition of safety risk

4.2.1 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 II*** to this Advisory Circular also has this provision.

4.3 Safety risk probability

4.3.1 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 or frequency that a safety consequence or outcome might occur. The determination of likelihood can be aided by questions such as:

4.3.1.1 Is there a history of occurrences similar to the one under consideration, or is this an isolated occurrence?
4.3.1.2 What other equipment or components of the same type might have similar defects?

4.3.1.3 How many personnel are following, or are subject to, the procedures in question?

4.3.1.4 What percentage of the time is the suspect equipment or the questionable procedure in use?

4.3.1.5 To what extent are there organizational, managerial or regulatory implications that might reflect larger threats to public safety?

4.3.2 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.

4.3.3 Table 2 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.

4.3.4 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 2: Safety risk probability table

Risk Probability	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

4.4 Safety Risk Severity

4.4.1 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 assessment can be based upon:

4.4.1.1 Fatalities/injury.

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

4.4.1.2 Damage.

(a) What is the likely extent of aircraft, property or equipment damage? i.e. damage or structural failure sustained by the aircraft which adversely affects the structural strength, performance or flight characteristics of the aircraft OR 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.

4.4.2 The severity assessment should consider all possible consequences related to an unsafe condition or object, taking into account the worst foreseeable situation. Table 3, 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 3: 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

4.5 Safety risk tolerability

4.5.1 The safety risk probability and severity assessment process is used to derive a safety risk index. The index created through the methodology described 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 4.

4.5.2 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 4: Safety Risk Assessment Matrix

Safety Risk		*Severity*				
Probability		*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")

4.5.3 The index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix {Table 5 (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 "intolerable category". In this case, the safety risk index of the consequence is unacceptable. The organization must therefore take measures to reduce:

4.5.3.1 the organization's exposure to the particular risk, i.e. reduce the likelihood component of the risk index;

4.5.3.2 the severity of consequences related to the hazard, i.e. reduce the severity component of the risk index; or

4.5.3.3 both the severity and probability so that the risk is managed to an acceptable level.

Note:— The inverted pyramid in Table 5(b) reflects a constant effort to drive the risk index towards the bottom APEX of the pyramid. Table 6 provides an example of an alternate safety risk tolerability matrix.

Table 5 (a): Safety Risk Tolerability Matrix

Safety Risk 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 5 (b)

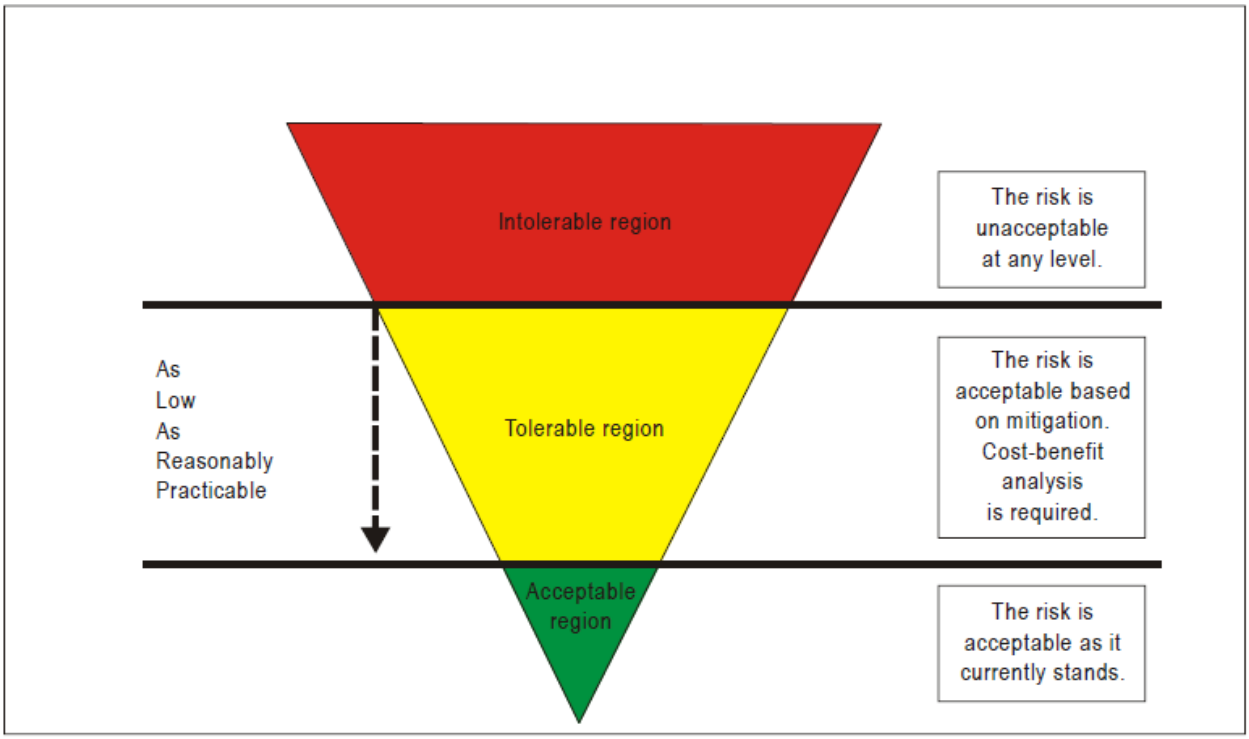


Table 6: An Alternate Safety Risk Tolerability Matrix

Risk Index range	Description	Recommended action
5A, 5B, 5C, 4A, 4B,3A	**High risk**	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	**Moderate risk**	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	**Low risk**	Acceptable as is. No further risk mitigation required

4.6 Human Factors related risks

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

4.6.1.1 contributing to an accident or incident through variable performance due to human limitations;

4.6.1.2 anticipating and taking appropriate actions to avoid a hazardous situation: and

4.6.1.3 solving problems, making decisions and taking actions to mitigate risks.

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

5.0 SAFETY RISK MITIGATION

5.1 General Principles

5.1.1 After safety risks have been assessed through the preceding step, elimination and/or mitigation to an acceptable level must take place. This is known as safety risk mitigation.

5.1.2 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.

5.1.3 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

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

5.2.1.1 Avoidance.

(a) 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.

5.2.1.2 Reduction.

(a) 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.

5.2.1.3 Segregation of Exposure.

(a) 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.

5.2.2 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 should be examined from the following perspectives:

5.2.2.1 *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.

5.2.2.2 *Cost/benefit*. The extent to which the perceived benefits of the mitigation outweighs the costs.

5.2.2.3 *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.

5.2.2.4 *Acceptability*. The extent to which the alternative is acceptable to those people that will be expected to apply it.

5.2.3 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:

5.2.3.1 technology;

5.2.3.2 training; and

5.2.3.3 regulations.

5.2.4 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:

5.2.4.1 existing defences protect against the safety risks;

5.2.4.2 defences function as intended;

5.2.4.3 the defences are practical for use under working conditions;

5.2.4.4 staff are aware of safety risks of the consequences of the hazard and the defences in place;

5.2.4.5 additional safety risk mitigation and control measures are required.

6.0 SAFETY RISK ACCEPTANCE

6.1 General Principles

6.1.1 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 service provider level.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.2 Human factors and risk management

6.2.1 Given that mature SSPs and SMSs target both human and organizational factors, a specific analysis process is a component of any mature, effective risk management system. In the course of any hazard identification and risk mitigation exercise involving human elements, it is necessary to assure that existing or recommended defences have taken Human Factors (HF) into consideration.

6.2.2 Where necessary, a supplementary HF analysis may be conducted to support that particular risk mitigation exercise/team. An HF analysis provides an understanding of the impact of human error on the situation and ultimately contributes to the development of more comprehensive and effective mitigation/corrective actions.

6.2.3 A human error model is the basis of the analysis process, and it defines the relationship between performance and errors and categorizes errors to permit the root hazards to be more readily identified and better understood. This understanding ensures the adequate completion of a root-cause analysis. Individual actions and decisions viewed out of context can appear to be virtually random events, escaping their due attention.

6.2.4 Human behaviour is not necessarily random. It usually conforms to some pattern and can be analysed and properly understood. Ultimately, this important HF perspective results in a more comprehensive and in-depth mitigation process.

6.2.5 The HF analysis ensures that during the organization's risk mitigation process, when identifying root, contributory or escalation factors; human factors and their associated circumstantial, supervisory and organizational impacts are duly taken into consideration.

6.3 Cost-Benefit Analysis (CBA)

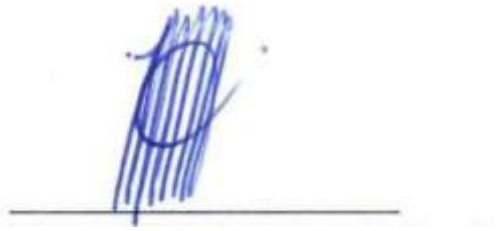
6.3.1 Cost-benefit Analysis (Cost Effectiveness Analysis) is normally an independent process from safety risk mitigation or assessment. It is commonly associated with a higher level management protocol, such as a regulatory impact assessment or business expansion project. However, there may be situations 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.

6.4 Safety Risk management documentation

6.4.1 Safety risk management activities should be documented, including any assumptions underlying the probability and severity assessment, decisions made, and any safety risk mitigation actions taken. This may be done using a spread sheet or table. Some organizations may use a database or

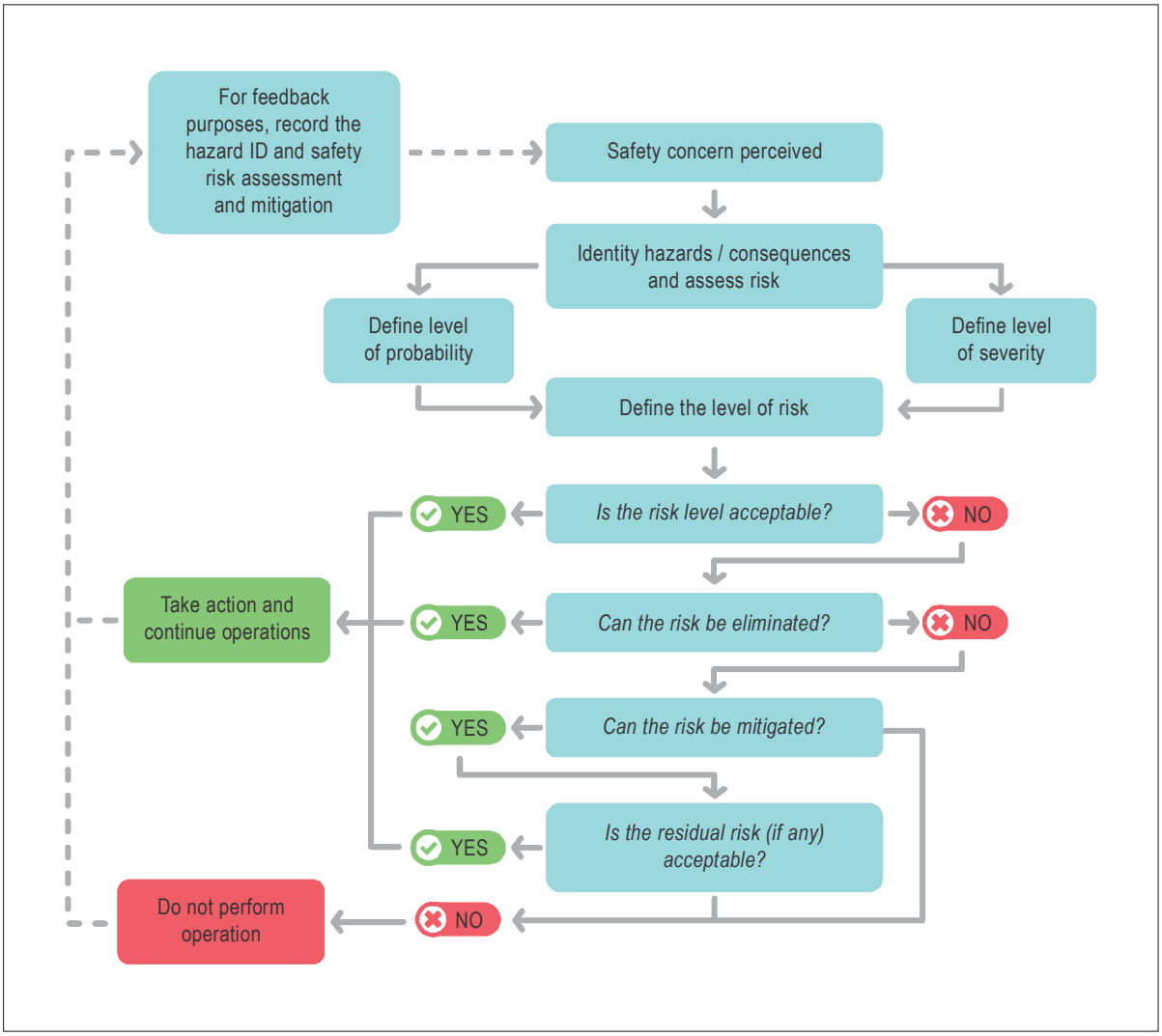
other software where large amounts of safety data and safety information can be stored and analysed.

6.4.2 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 ***(Appendix 1).***



CIVIL AVIATION AUTHORITY

SAFETY RISK MANAGEMENT DECISION AID.



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.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

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)	

TABLE D- SEVERITY TABLE (BASIC)

Level	*Descriptor*	*Severity description (customize according to the nature of the product or the service provider's operations)*
1	Insignificant	No significance to aircraft-related operational safety
2	Minor	Degrades or affects normal aircraft operational procedures or performance
3	Moderate	Partial loss of significant/major aircraft systems or results in abnormal application of flight operations procedures
4	Major	Complete failure of significant/major aircraft systems or results in emergency application of flight operations procedures
5	Catastrophic	Loss of aircraft or lives

TABLE E- SEVERITY TABLE (ALTERNATE)

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*
1	Insignificant	No significance to aircraft-related operational safety	No injury	No damage	No revenue loss	No effect	No implication
2	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
3	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
4	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
5	Catastrophic	Aircraft/hull loss	Multiple fatality	Catastrophic damage More than $__	Massive loss More than $__	Massive effect	International implication

TABLE F- LIKELIHOOD TABLE

Level	*Descriptor*	*Likelihood description*
A	Certain/frequent	Is expected to occur in most circumstances
B	Likely/occasional	Will probably occur at some time
C	Possible/remote	Might occur at some time
D	Unlikely/improbable	Could occur at some time
E	Exceptional	May occur only in exceptional circumstances

,

TABLE G- RISK INDEX MATRIX (SEVERITY x LIKELIHOOD)

Likelihood	*Severity*				
	1. Insignificant	*2. Minor*	*3. Moderate*	*4. Major*	*5. Catastrophic*
A. Certain/frequent	Moderate (1A)	Moderate (2A)	High (3A)	Extreme (4A)	Extreme (5A)
B. Likely/occasional	Low (1B)	Moderate (2B)	Moderate (3B)	High (4B)	Extreme (5B)
C. Possible/remote	Low (1C)	Low (2C)	Moderate (3C)	Moderate (4C)	High (5C)
D. Unlikely/improbable	Negligible (1D)	Low (2D)	Low (3D)	Moderate (4D)	Moderate (5D)
E. Exceptional	Negligible (1E)	Negligible (2E)	Low (3E)	Low (4E)	Moderate (5E)

TABLE H - RISK ACCEPTABILITY (TOLERABILITY) TABLE

Risk Index	*Tolerability*	*Action required (customize as appropriate)*
5A, 5B, 4A	Extreme risk	Stop operation or process immediately. Unacceptable under the existing circumstances. Do not permit any operation until sufficient control measures have been implemented to reduce the risk to an acceptable level. Top management approval required.
5C, 4B, 3A	High risk	Caution. Ensure that risk assessment has been satisfactorily completed and declared preventive controls are in place. Senior management approval of risk assessment before commencement of the operation or process.
1A, 2A, 2B, 3B, 3C, 4C, 4D, 5D, 5E	Moderate risk	Perform or review risk mitigation as necessary. Departmental approval of risk assessment.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Low risk	Risk mitigation or review is optional.
1D, 1E, 2E	Negligible risk	Acceptable as is. No risk mitigation required.