



Civil Aviation Authority of Sri Lanka

SAFETY RISK ASSESSMENT MANUAL

First Edition 2010


Issued under the authority of the Director General of Civil Aviation

Rev 00	Civil Aviation Authority of Sri Lanka	Date : 04 Oct 2010
--------	---------------------------------------	--------------------



SAFETY RISK ASSESSMENT

Control Number – 001

	Safety Risk Assessment Manual	SLCAP 2500
		Page: ii

Forward

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 and those safety risks the control and mitigation of which are viable.

The service providers operating in accordance with the requirements contained in ICAO Annex 11 - *Air Traffic Services*, Annex 14 - *Aerodromes, Volume I - Aerodrome Design and Operations*, ICAO Annex 6 - *Operation of Aircraft, Part I - International Commercial Air Transport - Aeroplanes, and Part III - International Operations - Helicopters* shall implement a Safety Management System in accordance with the requirements given in the ASN 92.

Further as per the requirements of the ASN 92, 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.

H.M.C. Nimalsiri
Director General of Civil Aviation &
Chief Executive Officer

04th Oct. 2010

Rev 00	Civil Aviation Authority of Sri Lanka	Date : 04 Oct 2010
--------	---------------------------------------	--------------------




List of Effective Pages

Page	Eff. Date	Page	Eff. Date	Page	Eff. Date	Page	Eff. Date
1-1	04.10.2010						
1-2	04.10.2010						
2-1	04.10.2010						
2-2	04.10.2010						
2-3	04.10.2010						
2-4	04.10.2010						
3-1	04.10.2010						
3-2	04.10.2010						
4-1	04.10.2010						
4-2	04.10.2010						
5-1	04.10.2010						
5-2	04.10.2010						
6-1	04.10.2010						
6-2	04.10.2010						
6-3	04.10.2010						
6-4	04.10.2010						
6-5	04.10.2010						



Table of Contents

FORWARD	II
LIST OF EFFECTIVE PAGES	III
RECORD OF AMENDMENTS	IV
TABLE OF CONTENTS	V
CHAPTER 1 – DEFINITION OF SAFETY RISK	1
CHAPTER 2 – FIRST FUNDAMENTAL — SAFETY RISK MANAGEMENT	1
CHAPTER 3 – SECOND FUNDAMENTAL — SAFETY RISK PROBABILITY	1
CHAPTER 4 – THIRD FUNDAMENTAL — SAFETY RISK SEVERITY	1
CHAPTER 5 – FOURTH FUNDAMENTAL — SAFETY RISK TOLERABILITY	1
CHAPTER 6 – FIFTH FUNDAMENTAL — SAFETY RISK CONTROL/MITIGATION	1

	Safety Risk Assessment Manual	SLCAP 2500	
	Definition of Risk	Chapter 1	Page: 1-1

Chapter 1 – Definition of Safety Risk


1.1 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.

1.2 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 analysed 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.

1.3 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.

1.4 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.

1.5 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

	Safety Risk Assessment Manual	SLCAP 2500	
	Definition of Risk	Chapter 1	Page: 1-2

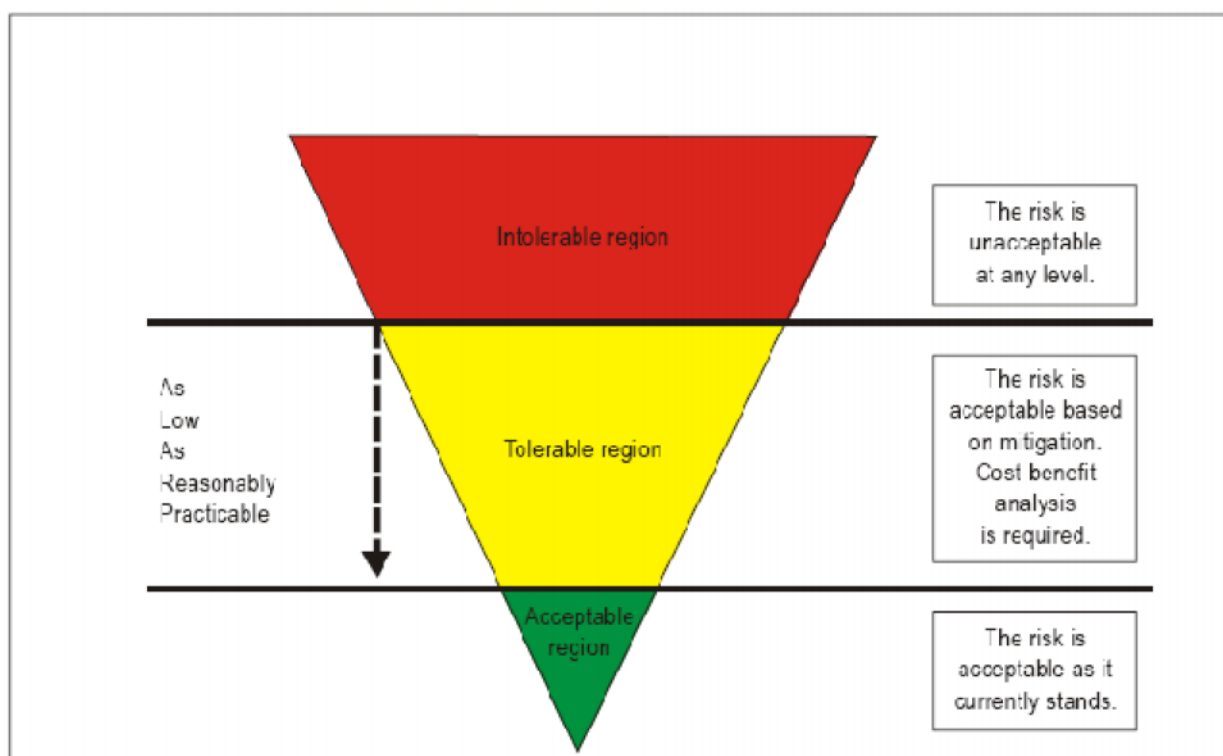
do not really exist in the natural world. Safety risk is a product of the human mind intended to measure the seriousness of, or “put a number” on, the consequences of hazards.

1.6 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.

Chapter 2 – First Fundamental — Safety Risk Management

2.1 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.

2.2 Figure 2-1 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.




	Safety Risk Assessment Manual	SLCAP 2500	
	First Fundamental – Safety Risk Management	Chapter 2	Page: 2-2

Figure 2-1 Safety risk management


2.3 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.

2.4 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?

2.5 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.

	Safety Risk Assessment Manual	SLCAP 2500	
	First Fundamental – Safety Risk Management	Chapter 2	Page: 2-3


2.6 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.

2.7 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 personnel to fly with an airline 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. Companies operating a one-of-a-kind aircraft may find that their spares inventory and the people specially trained for such an aircraft become surplus.
- 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


	Safety Risk Assessment Manual	SLCAP 2500	
	First Fundamental – Safety Risk Management	Chapter 2	Page: 2-4

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.

2.8 Cost-benefit analyses produce results that can be numerically precise and analytically exact. Nevertheless, there are less exact numeric factors that 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?

	Safety Risk Assessment Manual	SLCAP 2500	
	Second Fundamental – Safety Risk Probability	Chapter 3	Page: 3-1

Chapter 3 – Second Fundamental — Safety Risk Probability

3.1 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.

3.2 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?

3.3 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.


3.4 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.

3.5 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.

3.6 Figure 3-1 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.

	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 3-1. Safety risk probability table

	Safety Risk Assessment Manual	SLCAP 2500	
	Third Fundamental – Safety Risk Severity	Chapter 4	Page: 4-1

Chapter 4 – Third Fundamental — Safety Risk Severity

4.1 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.

4.2 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 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.

4.4 Figure 4-1 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 of occurrence	Meaning	Value
Catastrophic	<ul style="list-style-type: none"> — Equipment destroyed — Multiple deaths 	A
Hazardous	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — Nuisance — Operating limitations — Use of emergency procedures — Minor incident 	D
Negligible	<ul style="list-style-type: none"> — Little consequences 	E

Figure 4-1. Safety risk severity table

	Safety Risk Assessment Manual	SLCAP 2500	
	Fourth Fundamental – Safety Risk Tolerability	Chapter 5	Page: 5-1

Chapter 5 – Fourth Fundamental — Safety Risk Tolerability

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

5.2 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 5-1. 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 5-1 reflects the tolerability regions in the inverted triangle in Figure 2-1.

5.3 Second, the safety risk index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix that describes the tolerability criteria. The criterion for a safety risk assessed as 4B is, according to the tolerability table in Figure 5-2, “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 5-1. Safety risk assessment matrix

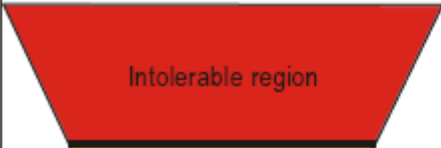



Suggested criteria	Assessment risk index	Suggested criteria
 Intolerable region	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
 Tolerable region	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable based on risk mitigation. It may require management decision.
 Acceptable region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

Figure 5-2. Safety risk tolerability matrix

	Safety Risk Assessment Manual	SLCAP 2500	
	Fifth Fundamental – Safety Risk Control/Mitigation	Chapter 6	Page: 6-1

Chapter 6 – Fifth Fundamental — Safety Risk Control/Mitigation

6.1 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.

6.2 Continuing with the example presented in chapter 5 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 6-1 presents the process of safety risk management in graphic format.

6.3 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.
- 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.

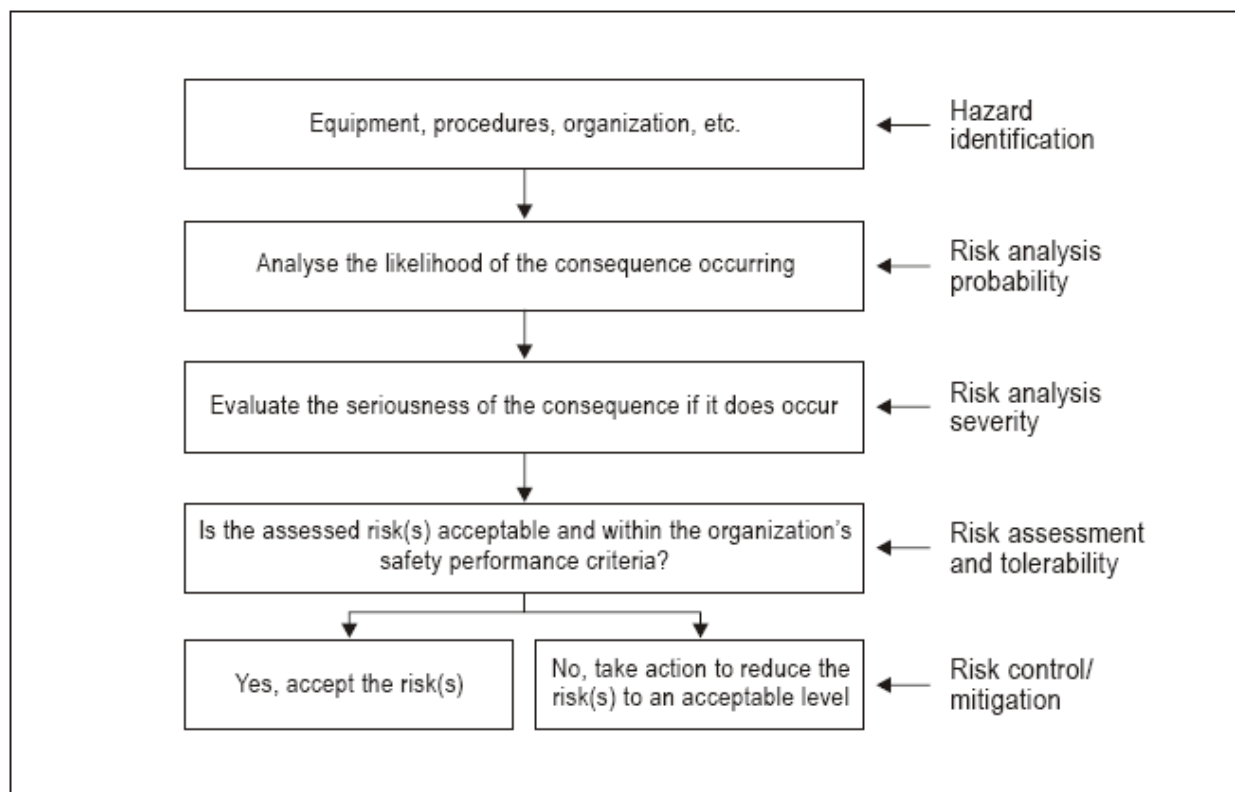



Figure 6-1. The process of safety risk management

6.4 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.

	Safety Risk Assessment Manual	SLCAP 2500	
	Fifth Fundamental – Safety Risk Control/Mitigation	Chapter 6	Page: 6-3

- 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?

6.8 Figure 6-2 presents the full safety risk/mitigation process in graphic format.

Rev 00	Civil Aviation Authority of Sri Lanka	Date : 04 Oct 2010
--------	---------------------------------------	--------------------

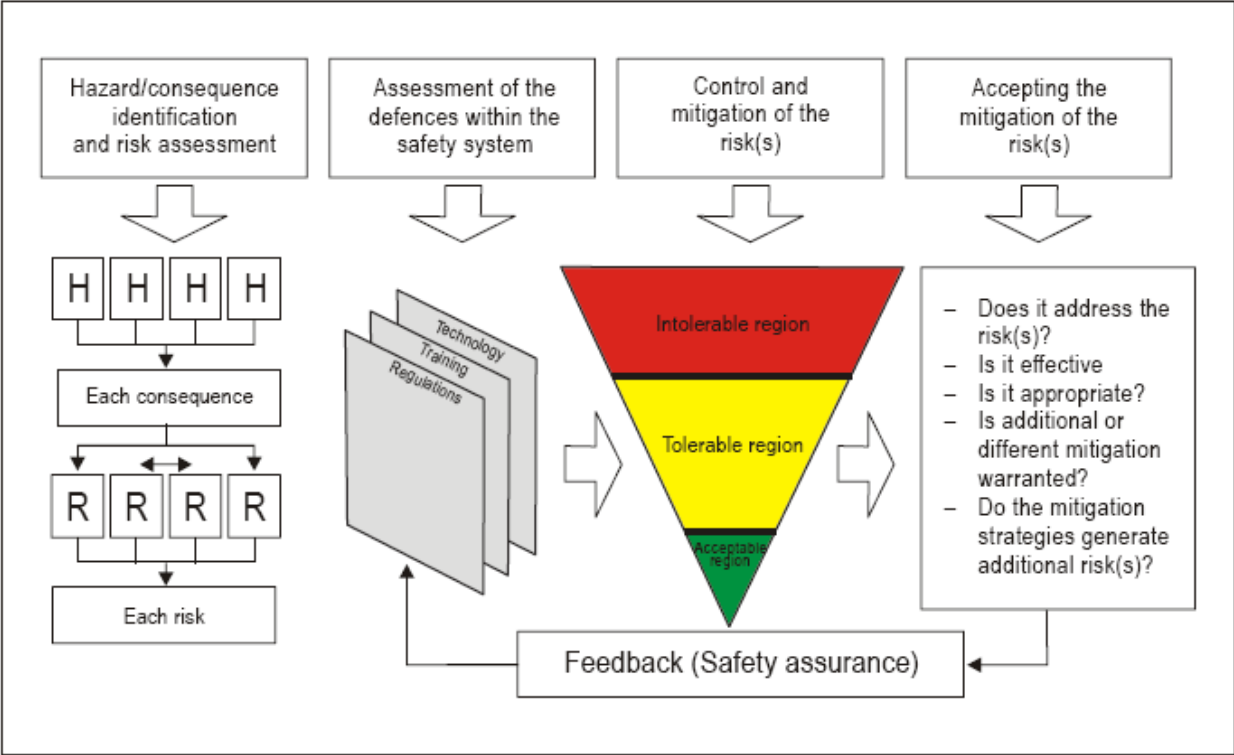


Figure 6-2. The safety risk mitigation process

Figure 6-3 presents the safety risk management process in its entirety.

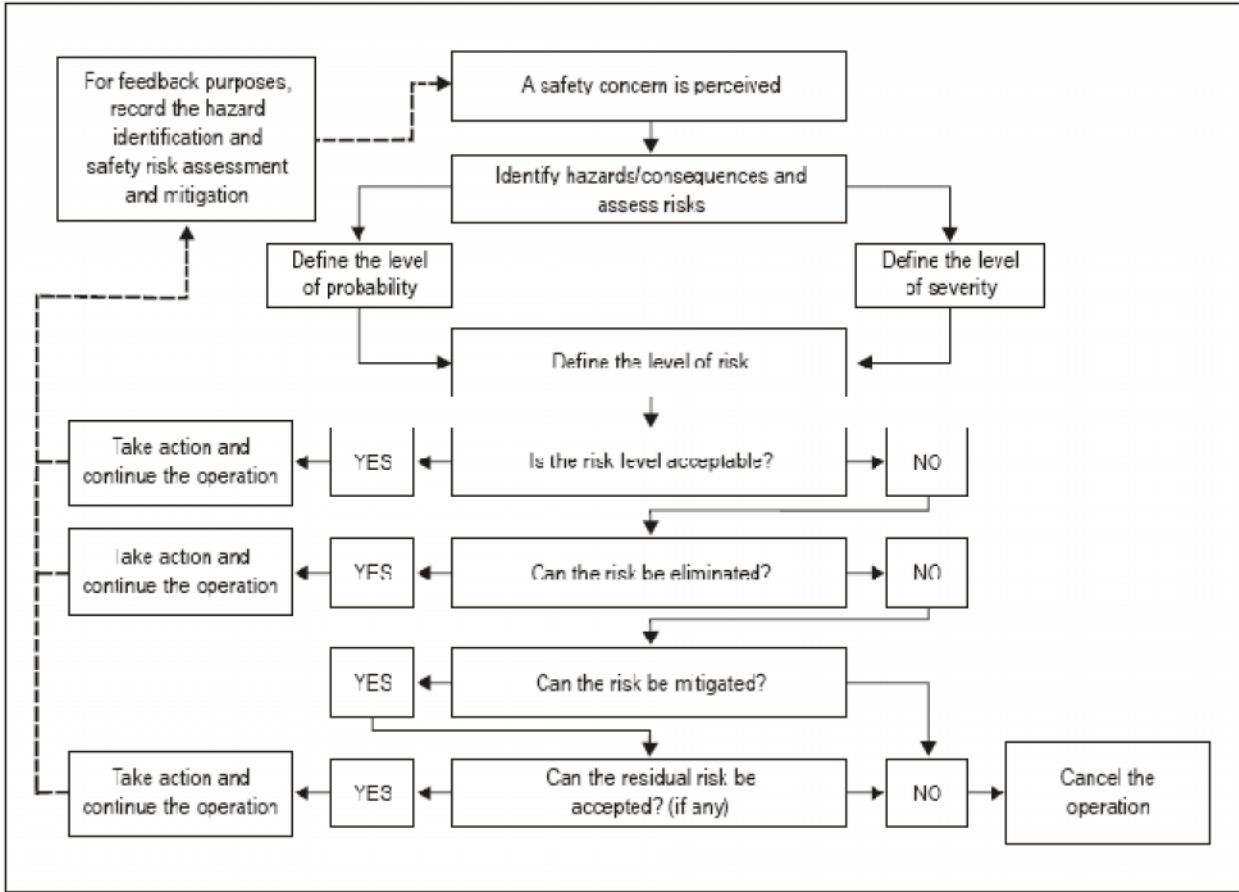


Figure 6-3. The safety risk management process