Safety Regulation Group

CAP 728

The Management of Safety

Guidance to Aerodromes and Air Traffic Service Units on the Development of Safety Management Systems

www.caa.co.uk

Safety Regulation Group

CAP 728

The Management of Safety

Guidance to Aerodromes and Air Traffic Service Units on the Development of Safety Management Systems

Important Note

The CAA has made many of the documents that it publishes available electronically (in addition to traditional printed format). Where practical, the opportunity has been taken to incorporate a clearer revised appearance to the documents. Any significant changes to the content of this document will be shown in the Explanatory Note. If no such changes are indicated the material contained in this document, although different in appearance to the previously printed version, is unchanged. Further information about these changes and the latest version of documents can be found at www.caa.co.uk.

28 March 2003

ISBN 0 86039 912 5

Issue 1, 28 March 2003

Enquiries regarding the content of this publication should be addressed to:
Aerodrome, Air Traffic and Licensing Standards Division, Safety Regulation Group, Civil Aviation Authority, Aviation House, Gatwick Airport South, West Sussex, RH6 0YR.

The latest version of this document is available in electronic format at www.caa.co.uk, where you may also register for e-mail notification of amendments.

Printed copies and amendment services are available from: Documedia Solutions Ltd., 37 Windsor Street, Cheltenham, Glos., GL52 2DG.

List of Effective Pages

Chapter	Page	Date	Chapter	Page	Date
	iii	28 March 2003			
	iv	28 March 2003			
	v	28 March 2003			
	vi	28 March 2003			
	vii	28 March 2003			
	viii	28 March 2003			
Chapter 1	1	28 March 2003			
Chapter 1	2	28 March 2003			
Chapter 2	1	28 March 2003			
Chapter 2	2	28 March 2003			
Chapter 2	3	28 March 2003			
Chapter 2	4	28 March 2003			
Chapter 3	1	28 March 2003			
Chapter 3	2	28 March 2003			
Chapter 3	3	28 March 2003			
Chapter 3	4	28 March 2003			
Chapter 4	1	28 March 2003			
Chapter 4	2	28 March 2003			
Chapter 4	3	28 March 2003			
Chapter 4	4	28 March 2003			
Chapter 4	5	28 March 2003			
Chapter 4	6	28 March 2003			
Chapter 5	1	28 March 2003			
Chapter 5	2	28 March 2003			
Chapter 5	3	28 March 2003			
Chapter 5	4	28 March 2003			
Chapter 5	5	28 March 2003			

Contents

Glossary of Commonly Used Terms and Definitions

1 Introduction

It is recognised that to achieve the shift towards safety management it is necessary that Safety Regulation Group (SRG) use a common language of safety where practicable. This chapter provides SRG with a standard set of safety management system terms and definitions.

Term	Definition	Source
A		
Accident	An unintended event or sequence of events that cause death, injury, environmental or material damage.	DEF STAN 00-55
C		
Competent Authority	Means in relation to the United Kingdom, the Authority, and in relation to any other country the authority responsible under the law of that country for promoting the safety of civil aviation.	ANO Art 118
Common Cause Failure	A failure which is the result of an event(s) which because of dependencies, cause a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to a defined system failing to perform its intended function.	IEC 1508
F		
Failure	A loss of function, or malfunction, of a system or part thereof.	JAR 25
H		
Harm	The loss to a human being or to a human population.	RBRA Task Team
Hazard	A physical situation, often following from some initiating event, that can lead to an accident.	DEF STAN 00-55 (and NATS)
I		
Inspection	An Inspection is the process of examining, checking or looking at a product or activity.	JAR 145 Derivation
L		
Level of Safety	A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable risk, based on the current values of society.	IEC 1508

Term	Definition	Source
Q		
Qualitative	Those analytical processes that assess system and aeroplane safety in a subjective, non-numerical manner	JAR 25
Quantitative	Those analytical processes that apply mathematical methods to assess system and aeroplane safety.	JAR 25
R		
Risk	Is the combination of the probability, or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence.	BS 4778
Risk Assessment	Assessment of the system or component to establish that the achieved risk level is lower than or equal to the tolerable risk level.	DEF STAN 00-56 & NATS
S		
Safety	Freedom from unacceptable risk of harm.	IEC 1508 & ISO/ IEC Guide 2 1986
Safety Assessment	A systematic, comprehensive evaluation of an implemented system to show that the safety requirements are met.	ARP4761
Safety Audit	A systematic and independent examination to determine whether safety related activities and related results comply with planned arrangements and whether these arrangements are suitable to achieve safety objectives and are implemented effectively	JAR 1 45 (Derivation)
Safety Case or Safety Assurance	A documented account of the evidence, arguments and assumptions to show that system hazards have been identified and controlled, both in engineering and operational areas, and that qualitative and quantitative safety requirements have been met.	NATS
Safety Objective	A safety objective is a planned and considered goal that has been set by a design or project authority.	CAP 670
Safety Policy	Defines the fundamental approach to managing safety and that is to be adopted within an organisation and its commitment to achieving safety.	NATS
Safety Requirements	The requirements for safety features to be met by a system.	Based on DEF STAN 00-55

Term	Definition	Source
Severity	The potential consequences of a hazard.	NATS
System	A combination of physical components, procedures and human resources organised to achieve a function.	NATS
V		
Validation	The evaluation of a system to ensure compliance with users' requirements. Note: Validation is generally used to refer to a larger process than verification. In particular, whereas verification test against specifications, validation is concerned with whether the operation of the system provides the results needed by the users. Validation therefore, includes the consideration of whether the specification of a system sufficiently and accurately represents the needs of the intended user.	NATS
Verification	The process of determining whether or not the product of each phase of the development process is consistent with the requirements specified in the previous phase.	NATS

Chapter 1 Introduction to Safety Management Systems (SMS)

1 Introduction

1.1 The primary objective of the Safety Regulation Group (SRG) is:

1.2 'To develop safety improvement concepts and a safety improvement action programme in partnership with industry to ensure that the frequency of fatal accidents does not increase in line with forecast growth in traffic and a consequent loss of public confidence'.

1.3 As part of this partnership the Aerodrome and Air Traffic Standards Division (AATSD) of the Civil Aviation Authority Safety Regulation Group has developed this document in order to provide guidance to industry on how to develop and adopt a system for managing safety. A positive benefit of this approach is to encourage a shift in the safety culture of the Industry. The document also provides necessary guidance on the implementation of a complementary audit based approach to safety regulation by SRG.

2 Document Structure

This document includes the following elements:

Glossary:	Commonly used terms and definitions
Chapter 1:	This Overview of the document
Chapter 2:	Safety Management Policy and Strategy
Chapter 3:	Safety Assurance Documentation
Chapter 4:	Risk Assessment Methodology
Chapter 5:	Safety Auditing of an Organisation

3 Objective of this document.

- To indicate to the aerodrome and air traffic service industry the core principles for the management of safety.
- To encourage all licenced aerodromes and air traffic service units (ATSUs) to review their existing operational safety management arrangements and develop and document robust procedures.
- To provide guidance on the structure and content of safety assurance documentation appropriate to the aerodrome and ATSU environment.
- To provide information to Industry on SRG's approach to safety regulatory auditing.

4 Scope

The material contained in this document is applicable to all licensed aerodromes and approved Air Traffic Service Units in the United Kingdom.

5 Comments on this document

5.1 The AATSD is committed to working with those we regulate in order to ensure that the requirements and guidance material which evolve are practical and achievable.

5.2 All comments received as a result of the publication of this document will be considered and a response forwarded to the correspondent. Where the comments are found to be valid the document will be amended prior to formal publication. A record of all comments received together with responses and subsequent actions will be made available on request.

Chapter 2 Safety Management Policy and Strategy

1 Introduction

This chapter provides a set of generic Safety Management Policies and Strategy which will form the basis of an effective method of managing safety.

2 Safety Management

2.1 Safety Management is that part of the overall management function which determines and implements an organisation's safety policy.

2.2 The implementation of a safety management system by an organisation should be endorsed by the most senior level of management within the organisation and follow a logical programme which ensures that:

- Safety policy statements should define the organisation's fundamental approach to the management of safety and should commit the organisation at all levels to the fulfilment of its stated safety policy.
- From the policy statements the organisation should define its safety management strategy.
- Having defined the policy statements and the organisation's strategy the procedures designed to achieve this should be clearly documented.
- The responsibilities and accountabilities of all individuals in respect of safety should be clearly defined.

3 Safety Management Policy Statements

The Policy Statements should define the fundamental approach to be adopted for managing safety and the organisation's commitment to safety.

The following should be considered as essential elements of safety management policy.

3.1 Safety Objective

Rationale: This should be the key policy statement defining what the organisation is striving to achieve through its safety management system.

The organisation should state a top-level commitment to a business objective for safety that minimises its contribution to aviation accident risk to as low as reasonably practicable.

NOTE: Where risk is concerned there is no such thing as absolute safety. "As low as reasonably practicable" means that risk in a particular activity can be balanced against the time, cost and difficulty of taking measures to avoid the risk. The greater the risk to safety, the more likely it is that it is reasonable to go to substantial effort to reduce it. It is implicit, therefore, that hazards have to be identified and the risk assessed before a judgement can be made upon their tolerability.

3.2 Safety Management

Rationale: An intuitive or ad hoc approach to safety is not acceptable.

The organisation should make a commitment to the adoption of an explicit, pro-active approach to systematic safety management.

3.3 Safety Responsibility

Rationale: The safety management system depends upon individuals understanding and accepting their delegated responsibility within the organisation. Accountability for safety belongs to all levels of management and the attainment of satisfactory safety performance requires the commitment and participation of all members of the organisation. Everybody within an organisation should be made aware of the consequences of mistakes and strive to avoid them. Management should foster this basic motivation within members of an organisation so that everybody accepts their responsibility for safety.

The organisation should make a safety policy statement that confirms that everyone has an individual responsibility for the safety of their own actions and that managers are accountable for the safety performance of the activities for which they have responsibility. Additionally, the organisation should identify who is ultimately accountable for safety and how that accountability is delegated.

3.4 Safety Priority

Rationale: The safety management system should clearly address and resist misguided business pressures. Conversely, the safety management system should ensure that safety is not used to support commercial, financial, environmental etc. decisions inappropriately, which have little real safety significance. If the term 'safety' is abused in this way the safety management system cannot be focused on controlling the real risks.

The organisation should make a safety policy statement committing it to ensuring that the consideration of safety is given the highest priority when assessing commercial, operational, environmental or social pressures.

3.5 Safety Standards and Compliance

Rationale: Adopting minimum standards may not always achieve the organisation's safety objectives. Compliance with safety standards and requirements can form part of a robust safety argument and facilitates the safety assessment process.

The organisation should make a safety policy statement committing it, as a minimum, to complying with all appropriate safety standards and requirements.

3.6 Externally Supplied Products and Services

Rationale: A safety assessment requires input from all phases of a product or service development. For externally supplied products or services the external supplier must understand and comply with the organisation's safety and safety management system requirements.

The organisation should make a safety policy statement committing it to ensuring that the safety assurance processes used by its external suppliers satisfy its own safety management standards and safety requirements.

4 Safety Management Strategy

The following strategy reflects current best practice in the management of safety. It provides a framework for the establishment of processes to identify safety shortcomings, so that remedial action can be taken, and provide assurance that safety levels are being met or improved.

There are three basic principles to be applied:

- Safety Achievement: specifying the means by which the safety performance of the organisation meets its safety objectives and their derived requirements.
- Safety Assurance: specifying the means for providing assurance that risks are being managed properly and effectively.
- Safety Promotion: specifying the means by which safety issues are communicated within an organisation to eliminate unnecessary risks and avoid repeat errors or risks.

4.1 Safety Achievement

4.1.1 Level of Safety

Rationale: If the safety performance of a service or product is to be assessed and monitored it is necessary to define the safety objectives that need to be met.

The level of safety that the organisation seeks to achieve should be defined. This may take the form of statements identifying hazardous activities undertaken by the organisation and the safety performance required in that area.

4.1.2 System Safety Assessment

Rationale: A safety analysis process should be conducted to establish the appropriate safety requirements are established. The safety assessment process may identify hazards that do not, at present, satisfy the safety requirements.

An organisation should assess all existing operations, and proposed changes, additions or replacements, for their safety significance.

Where a hazard is identified, safety assurance is required. A safety assessment should be conducted and the results documented to ensure that full consideration is given to all aspects which may effect the safety of aircraft.

4.1.3 System Safety Assessment Records

Rationale: The results of the safety assessment should provide evidence to the organisation (and other parties) that it meets and continues to meet its safety objectives.

An organisation should record the safety requirements for its area of activity and the results of the safety assessment process.

4.1.4 Competency

Rationale: Staff competence is fundamental to safety.

The organisation should ensure that staff are competent and qualified for their role and responsibilities and remain so.

4.2 Safety Assurance

4.2.1 Safety Audits

Rationale: A safety audit is a pro-active safety management mechanism by which any risks within the organisation's operation are identified and controlled.

Organisations should routinely carry out safety audits to provide management with assurance that their operation meets the objectives of their safety management system and remains safe.

4.2.2 Performance Monitoring

Rationale: Safety performance can deteriorate, or the operational environment can change over time. Such events need to be detected and managed to ensure that the organisation continues to meet its safety objectives.

An organisation should have in place suitable monitoring arrangements so that undesirable trends in safety performance can be recognised.

4.2.3 Safety Significant Occurrences

Rationale: If lessons are to be learnt and remedial action is to be taken promptly, safety occurrences need to be investigated in a timely manner by the organisation. This activity should be additional to any statutory reporting requirements.

The organisation should have in place a process for investigating potential safety significant occurrences, identifying any failures of the organisation's management of safety and to take corrective action if required.

4.3 Safety Promotion

4.3.1 Lesson Dissemination

Rationale: It is essential that lessons should be learned and then remembered, so that the chance of recurrence is reduced. Including the results of such lessons in training programmes will raise staff awareness levels.

The organisation should ensure that lessons learnt from hazardous occurrence investigations, and the case histories or experience gained both internally and from other organisations, are distributed widely and actioned to minimise the risk of recurrence.

4.3.2 Safety Improvement

Rationale: This requires an effective means of communicating safety issues and the development of an internal safety culture that encourages every member of staff to focus on the achievement of safety, and to report errors and deficiencies without fear of punitive actions against them.

The organisation should have in place arrangements that actively encourage staff to identify potential hazards and propose solutions. The organisation should make appropriate changes, in respect of identified hazards, where safety can be improved.

Chapter 3 Safety Assurance Documentation (SAD)

1 Introduction

1.1 An effective Safety Management Policy and strategy require that an organisation should assess all existing operations, and proposed changes, additions or replacements, for their safety significance. Where a hazard is identified, safety assurance is required.

1.2 Assessments, their results and the subsequent procedures put in place to make sure that the necessary safety objectives are achieved, should be documented.

1.3 This safety assurance documentation can take many forms and is often referred by different names. The underlying principles behind the documentation and the information it contains are, however, common. The ATS Standards Department typically uses the term Safety Case although the same function may be satisfied by the Aerodrome Manual or an exposition.

1.4 Irrespective of the manner in which it is presented, a safety assurance document (SAD) should contain argument and evidence that the operation meets or exceeds the appropriate standard of safety.

1.5 This chapter provides guidance on the typical content and structure of a SAD which is acceptable to SRG and may form the basis of gaining and maintaining regulatory approval.

2 Content

2.1 Document Identification

A SAD should have a unique and clearly identifiable title.

2.2 Document Control

2.2.1 A system which ensures that the status of the documentation can be ascertained should be implemented. This can usually be achieved by a version numbering scheme. It is important to clearly indicate whether a document is in draft form and provide a point of contact able to confirm the validity of the version number.

2.2.2 It is useful to include a revision history whilst the document is under development.

2.3 Scope

2.3.1 The scope should identify what elements of the organisation's system are covered by the SAD. The boundaries of the system under consideration should be stated where possible and interfaces with other organisations identified.

2.3.2 Any assumptions made during the preparation of the SAD should be recorded.

2.3.3 Clearly, for the SAD to be suitable as a basis for regulatory approval the scope should be as comprehensive as possible.

2.4 System Description

2.4.1 The system encompassed by the SAD should be described in sufficient detail to enable the reader to understand the context in which the safety management processes described in the document are to be applied.

2.4.2 Ideally, discrete operating functions within the system should be identified and the broad inter-relationships between these functions described. An airport SAD, for example, might comprise the discrete functions of passenger handling within terminals, apron operations, aircraft fuelling, airside engineering and air traffic services. In this example, one would expect there to be liaison (an interface) between terminal and apron staff to ensure that passengers are not endangered, and so on.

2.5 Objectives

2.5.1 Applicable safety and regulatory requirements should be stated. These statements may include safety requirements derived from the organisation's safety policy, national and international Standards or Codes of Practice and regulatory requirements published by CAA.

2.5.2 It should be recognised that as the SAD is developed other safety requirements are likely to be identified.

2.6 Hazard Identification

2.6.1 Each operating function encompassed by the SAD is likely to involve a variety of systems (people, procedures, equipment or combinations of these) that support its activities.

2.6.2 The ways in which these systems can fail need to be considered and the resulting hazards identified.

2.7 Safety Assessment

2.7.1 Having identified the hazards that can occur, it is necessary to consider:

i) the seriousness (often referred to as severity) of the consequences should that failure occur; and

ii) the likelihood (probability) that the failure will occur.

NOTE: Risk is the product of the severity of an event and the probability of occurrence. A hazard which has serious consequences and which is likely to occur represents a high risk whereas a hazard of little consequence which is unlikely to occur represents a minimal risk.

2.7.2 Following this analysis, arguments should be devised and evidence presented that provide assurance that the management of these hazards is commensurate with the risk involved and the safety objectives which have been identified.

NOTE: These arguments may utilise previous performance data, engineered system design practices, current incident rates, competence criterion for personnel etc.

2.7.3 Hazard Identification and Safety Assessment are described in more detail in the Chapter 4.

2.8 Performance Measurement

2.8.1 It is necessary to ensure that the measures which are expected to assure safe operation do, in fact, do so.

2.8.2 The safety performance of the operation needs to be monitored, both proactively and reactively, to ensure that an acceptable level of safety continues to be achieved. A description of how the results of this safety performance monitoring will be used as feedback to improve the system should be included.

2.8.3 The organisation's safety management strategy will usually describe this process and may be referenced in the SAD. Some performance indicators, however, may be specific to the scope under consideration and may be described in detail in the SAD.

2.9 Safety Accountabilities

The safety accountabilities of all personnel should be defined and documented to explain how these safety significant roles are undertaken.

2.10 Safety Communications

2.10.1 The SAD should describe the methods used within the organisation to ensure that safety concerns are highlighted and communicated to those accountable for safety.

2.10.2 The means by which any lessons learned from the investigation of such safety concerns are disseminated should also be stated.

3 Structure

3.1 Application of a Safety Assurance Document

The scope of a SAD usually reflects one of two situations:

i) the safety of the existing, ongoing, operation of the aerodrome or ATSU (or sometimes just a particular part of the operation); or

ii) a change to the existing operation.

3.2 Association with a Safety Management Strategy

3.2.1 Although desirable, it is not essential for an organisation to have a documented Safety Management Strategy in place in order to develop a SAD. Where a Strategy exists, the SAD can make reference to already documented procedures that will be used in the safety assurance process. In the absence of a documented Strategy, the SAD will need to describe these processes in detail.

3.2.2 A comprehensive set of documents comprising a SAD represents the tangible product of an effective Safety Management System. The information included will provide those responsible for operational safety management with the detail necessary to undertake their safety responsibilities and will provide a baseline for audit.

3.3 Document Presentation

3.3.1 Where the SAD describes existing, ongoing, operations, a single living document (albeit referencing other documents) can usually be used to provide suitable argument and evidence for safety. Any changes to the documented system should, of course, be subject to the same safety analysis and the SAD amended if appropriate.

3.3.2 Where the SAD is used to describe a change to existing operations, it may not initially be possible to provide all the safety argument and evidence required. Examples of projects for which SAD might be prepared might include:

- the construction and introduction to service of a new taxiway
- changes to an apron road scheme
- the installation and commissioning of a replacement radar system
- the introduction of a new aircraft type or class
- the introduction of a new ATS procedure

3.3.3 Many large projects have distinct phases such as requirements definition, design evaluation, introduction to service and routine operation. The SAD can be presented in parts corresponding to these phases, as information becomes available.

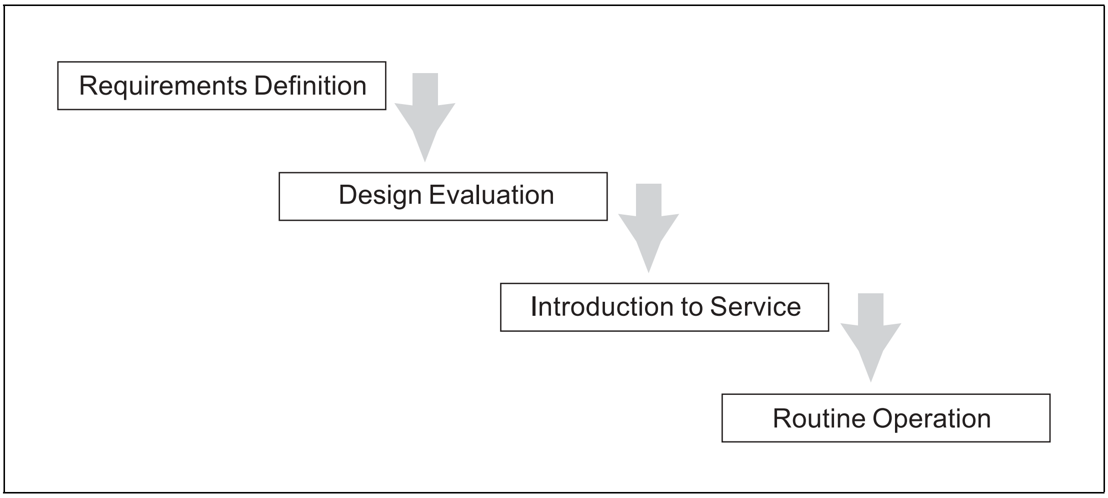


Figure 1 Typical project lifecycle phases and Safety Assurance Document parts

3.3.4 The component parts of the SAD, when the project is complete, should provide all the key elements described in Paragraph 2.

4 Associated Documentation and Procedures

Particularly where the SAD is considering a change to an existing system, other documents and procedures will be required to ensure safe operation. These may include Managing Director's Instructions, contractor's briefing notes and ATC Temporary Operating Instructions. That these documents will be produced will form part of the safety argument and, ideally, will be included in the SAD.

5 Interface with other Organisations

The SAD will have identified interfaces with third parties (handling agents or fuelling companies, for example) and any hazards which they may have some involvement with. Wherever possible the aerodrome authority or ATSU should formalise the interface and document the safety responsibilities of each organisation.

Chapter 4 Safety Assessment Methodology

1 Introduction

1.1 The chapter on Safety Management Policy and Strategy requires that an organisation should assess all aspects of its operation, and changes to it, for safety significance. Safety Assessments should be performed and documented to ensure that due consideration is given to the safety of all parts of the system.

1.2 The Safety Assessment should be conducted to ensure that the management of any hazards is commensurate with the risk involved and the safety objectives which have been identified.

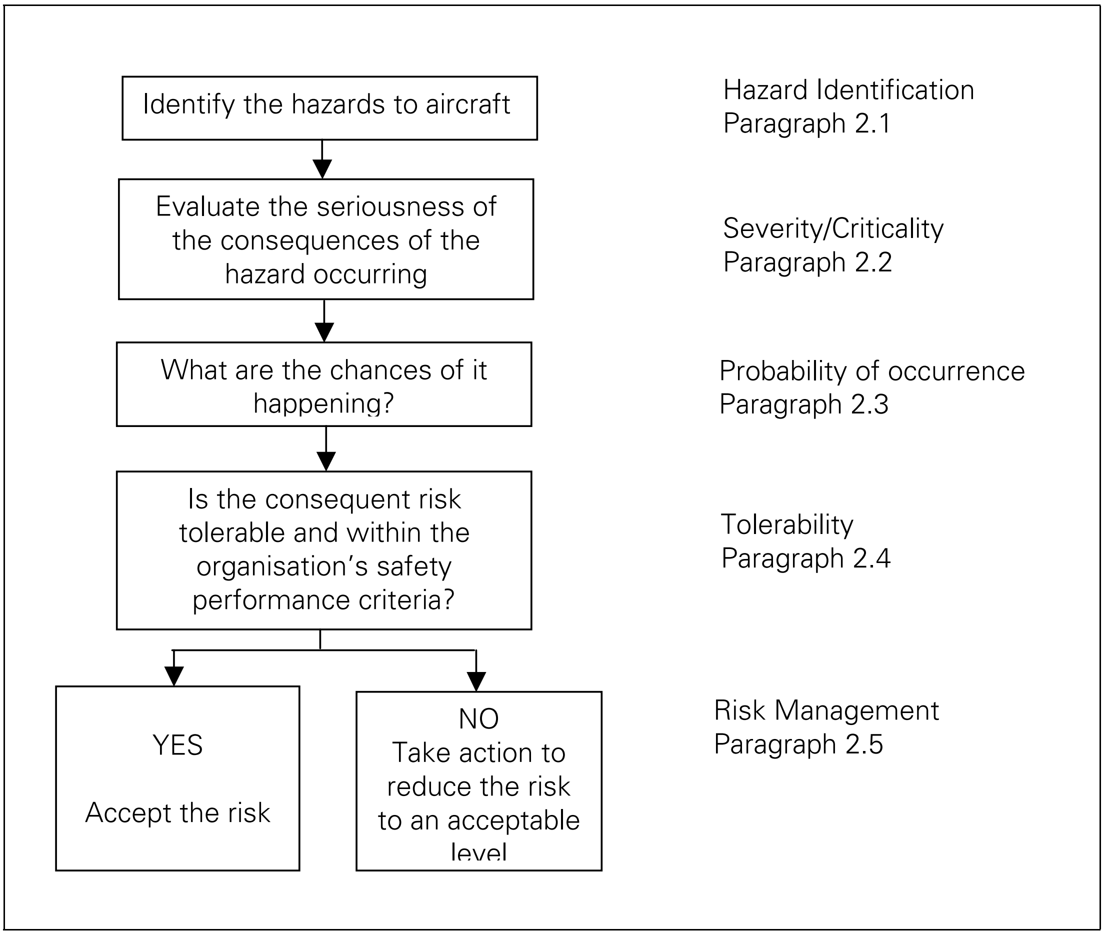
2 **Risk Management Process.** The generic process is as follows and is illustrated in the flow chart below:

Systematically identify Possible Hazards to aircraft.

Evaluate the seriousness of the consequences of the hazard occurring.

Consider the chances of it happening.

Determine whether the consequent risk is tolerable and within the organisation's acceptable safety performance criteria. If not, take action to reduce the severity of the hazard or the probability of it arising to reduce the risk to a tolerable level.


Identify the hazards to aircraft
Hazard Identification Paragraph 2.1
Evaluate the seriousness of the consequences of the hazard occurring
Severity/Criticality Paragraph 2.2
What are the chances of it happening?
Probability of occurrence Paragraph 2.3
Is the consequent risk tolerable and within the organisation's safety performance criteria?
Tolerability Paragraph 2.4
YES Accept the risk
NO Take action to reduce the risk to an acceptable level
Risk Management Paragraph 2.5

2.1 **Hazard identification**

Initially, a high level assessment of the reasonably foreseeable hazards should be carried out. Suitable techniques might include:

- Checklists

  Review experience and available data from accidents, incidents or similar systems and draw up a hazard checklist. Checklists identify potentially hazardous areas which will require further detailed evaluation.

- Group Review

  This may be a true brainstorming session or may be based on a review of the checklist. The group should consist primarily of people with as wide a background as possible and chosen for their relevant experience and competence.

2.2 **Evaluate the seriousness of the consequences of the hazard occurring**

2.2.1 The consequence of each identified hazard occurring should be assessed for its effect on aircraft safety. Figure 4.1 provides one recognised safety criticality classification scheme (JAR 25).

2.2.2 Figure 4.2 expands this classification scheme into a form more appropriate to the ATS environments.

2.3 **Consider the chances of it happening**

2.3.1 The probability of occurrence can be defined in both qualitative and quantitative terms.

2.3.2 Numerical (quantitative) methods may be required to further support the analysis of systems which have the potential to produce catastrophic or hazardous results. For lower levels of classification of risk, qualitative methods will often produce valid and acceptable results.

2.3.3 It will be noted that many of the hazards identified are acceptably mitigated by the application of existing Standards, regulations, procedures or practices.

2.3.4 Figure 4.3 illustrates the relationship between qualitative and quantitative probability of occurrence.

2.4 **Determine whether the consequent risk is tolerable and within the organisation’s acceptable safety performance criteria?** Once the severity of a hazard has been assessed and the probability of it arising has been estimated, a judgement can be made on whether the consequent risk is acceptable or not and whether it can be further reduced at reasonable cost. Common sense dictates that a major consequence of an undesired event with a high probability of occurrence is unacceptable, however it may be tolerable if the probability of occurrence is very low although it may be undesirable. The process of judging tolerability of risks and the results can be presented in tabular form as illustrated in Figure 4.4.

2.5 **Actions to reduce the severity of the hazard or the probability of it arising to reduce the risk to a tolerable level (managing risks).** Where the table indicates that the risk is currently unacceptable, action must be taken to reduce the probability of occurrence and/or the severity of the hazard. If neither mitigating measure is available, the system clearly does not satisfy the safety objectives. In any process where judgement is applied there will be situations where the tolerability is not clearly defined. An issue which falls into this area of uncertainty is likely to require, before implementation, the endorsement of the individual ultimately accountable for safety within the organisation.

Figure 4.1 Safety Criticality Classification (JAR 25)

Classification	Catastrophic	Hazardous	Major	Minor
Results in one or more of the following effects	• the loss of the aircraft • multiple fatalities	• a large reduction in safety margins • physical distress or a workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely • serious injury or death of a relatively small proportion of the occupants	• a significant reduction in safety margins • a reduction in the ability of the flight crew to cope with adverse operating conditions as a result of increase in workload or as a result of conditions impairing their efficiency • injury to occupants	• nuisance • operating limitations: emergency procedures

NOTE: This table is included to illustrate one possible classification scheme. The actual classification used in a safety assessment must be indicated in the safety assurance document.

Figure 4.2 Safety Criticality Classification expanded for the ATS environment

Classification	Catastrophic[1]	Hazardous	Major	Minor	Negligible
Results in one or more of the following effects	• ATC issues instruction or information which can be expected to cause loss of one or more aircraft (no reasonable and reliable means exists for the aircrew to check the information or mitigate against the hazards) • continued safe flight or landing prevented	• the ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, completely unavailable • provision of instructions or information which may result in a critical near mid-air collision or a critical near collision with the ground • many losses of acceptable separation possible	• the ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, severely degraded or compromised (e.g. contingency measures required or controller workload significantly increased such that the probability of human error is increased) • the ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, completely unavailable • provision of instructions or information which may result in the separation between aircraft or aircraft and the ground being reduced below normal standards • No ATS action possible to support aircraft emergency	• the ATC separation service provided to aircraft that are airborne or are inside a runway protected area in one or more sectors is suddenly, and for a significant period of time, impaired • the ATC separation service provided to aircraft on the ground outside a runway protected area is suddenly, and for a significant period of time, severely degraded • ATS emergency support ability severely degraded	• no effect on ATC separation service provided to aircraft • Minimal effect on ATC separation service provided to aircraft on the ground outside a runway protected area • Minimal effect on ATS emergency support ability Negligible

[1] It is not obvious that such a severe failure mode exists with the current UK ATC practices and systems but it may be possible in the future

NOTE: This table is included to illustrate one possible classification scheme. The actual classification used in a safety assessment must be indicated in the safety assurance document.

Figure 4.3 Probability of occurrence definitions

Probability of Occurrence Classification	**Extremely improbable**	**Extremely remote**	**Remote**	**Reasonably probable**	**Frequent**
Qualitative definition	Should virtually never occur in the whole fleet life.	Unlikely to occur when considering several systems of the same type, but nevertheless, has to be considered as being possible.	Unlikely to occur during total operational life of each system but may occur several times when considering several systems of the same type.	May occur once or several times during operational life	May occur once during total operational life of a single system
Quantitative definition	$<10^{-9}$ per flight hour	10^{-7} to 10^{-9} per flight hour	10^{-5} to 10^{-7} per flight hour	10^{-3} to 10^{-5} per flight hour	1 to 10^{-3} per flight hour

The table above is reproduced from JAR 25 and is specifically related to the probability of an event occurring during flight. It is considered that the definitions are equally valid for aircraft movements at an aerodrome or aircraft flights through an ATC airspace sector.

NOTE: This table is included to illustrate one possible classification scheme. The actual classification used in a safety assessment must be indicated in the safety assurance document.

Figure 4.4 Example Tolerability Matrix

	Probability of Occurrence				
Severity	Extremely improbable	Extremely remote	Remote	Reasonably probable	Frequent
Catastrophic	Review	Unacceptable	Unacceptable	Unacceptable	Unacceptable
Hazardous	Review	Review	Unacceptable	Unacceptable	Unacceptable
Major	Acceptable	Review	Review	Review	Review
Minor	Acceptable	Acceptable	Acceptable	Acceptable	Review

NOTE: This table is included to illustrate one possible classification scheme. The actual classification used in a safety assessment must be indicated in the safety assurance document.

Chapter 5 Safety Auditing of an Organisation

1 Introduction

1.1 Having implemented a system to manage safety within an organisation, it is necessary to confirm that the processes and results of that system actually achieve their intent, in the case of an aerodrome or air traffic control service unit this will be compliance with the organisation's safety objectives.

1.2 Although this Chapter describes the auditing process that is applied by the Safety Regulation Group, the principles detailed represent good practice which may be adopted by organisations when carrying out internal safety audits.

1.3 A safety regulatory audit may comprise elements of both audit and inspection and will involve assessing compliance against requirements, safety management procedures and personnel competence where appropriate. Performance measurements and appraisals of safety assurance documentation are all part of the safety regulatory function.

1.4 It is important to note that a safety audit does not seek to examine every aspect of an organisation. A sample of the safety related activities are selected on each occasion and, provided that the findings are satisfactory, the Regulator can have confidence that the remaining activities are similarly satisfactory.

1.5 Audits may be carried out prior to the issue of a licence or grant of Approval by the Authority and to confirm ongoing compliance with the terms and requirements of such a licence or Approval.

1.6 Unless otherwise specified, references in this Chapter to regulation means safety regulation and references to the auditor means an auditor of the Safety Regulation Group.

2 Scope

2.1 Three elements of regulation are assessed in a safety regulatory audit regime:

- Surveillance of Compliance with requirements
- Areas & Degree of Risk and their effective management
- The Competence and Performance of those responsible for safety

2.2 Each of these are considered in both normal day to day operation and in any area or time of change.

3 Surveillance of Compliance

3.1 Standards

3.1.1 The auditor will ascertain that the appropriate international, national, or local safety standards have been identified and are complied with are complied with, both prior to any licence or approval issue and on a continuous basis throughout the duration of that licence or approval.

3.1.2 The standards/requirements may be established from International Standards and Recommended Practices published by the International Civil Aviation Organisation, EC directives, Acts of Parliament or Civil Aviation Authority requirements.

3.2 **Submission of evidence.** The auditor will require documentary evidence of regulatory compliance from an organisation in advance of the issue of a licence or grant of an approval and may request information at any time subsequently. Documentary evidence will usually take the form of a Safety Assurance Document.

3.3 **Acceptable Means of Compliance.** In some circumstances, the auditor may indicate acceptable means of compliance with regulatory requirements to organisations. It is important that the organisation should not simply accept these without considering their implications on safety. Organisations should be aware that the application of minimum standards, which an acceptable means of compliance is likely to describe, may not meet their identified safety requirements in all circumstances. Any identified risks that fall outside of the scope of the standards or regulatory requirements should be recorded and managed appropriately by the organisation.

4 Areas and Degree of Risk

4.1 **Risk Assessment.** In order to ensure that an organisation's activities continue to be adequately safe, procedures and processes with safety significance must be periodically reviewed in order to ensure that they continue to meet the organisation's safety objectives. The auditor may examine the records of such reviews and, of course, details of risk assessments carried out when the organisation is considering changes to its existing operation.

4.2 **Safety Audits.** The organisation will require to satisfy itself that its routine operation meets its safety objectives. This can be achieved by a number of methods but, usually, a system of internal audit is used. The safety regulatory auditor may examine the reports of internal audits and those of any third parties in which safety issues may be raised.

5 The Competence and Performance of those Responsible for Safety

5.1 **Licensing.** In some situations, for example the provision of an air traffic control service, individuals are required to hold a licence in order to perform certain functions. The auditor will accept licences issued by the Authority and other recognised agencies as an indication of the competency of the individual to undertake the tasks associated with the licence. The issue and renewal of individual licences does not necessarily, however, measure the competence of the individual in other roles undertaken within an organisation. For example, a licensed individual who is perfectly competent to undertake the tasks associated with the privileges of his/her licence may fail to perform effectively in an additional role as a manager.

5.2 Competency

5.2.1 The Air Navigation Order places an obligation on the Regulator to be satisfied with the competency of the aerodrome licensee or ATC Provider's organisation. The organisation should, in addition, have in place a mechanism for ensuring that all staff are adequately competent in safety related activities to meet its safety objectives.

5.2.2 The auditor will seek to confirm that the competence of key personnel remains adequate; failure to satisfy the auditor in this respect may result in the variation or withdrawal of the organisation's licence or approval. The auditor may also examine the organisation's procedures for assuring the competence of its own staff and, in cases where safety can be compromised, the staff of other organisations operating within the aerodrome environment. The auditor will take into account the culture generated by those with influence and power within the organisation.

5.2.3 Where an individual's competence is necessary for safe operation, the organisation will need to satisfy the auditor that suitable procedures are in place to manage any deficiency in staffing levels or other factor which may affect the organisation's ability to perform that function safely.

5.3 **Audit Responsibility.** Any safety audit (whether internal or external) should involve the highest level of management with responsibility for safety within the organisation. It is important that senior management are aware of the findings of safety audits in order that appropriate action can be taken. The auditor may assess management's involvement in the day to day safety of the organisation through this means.

6 Performance Indicators

6.1 Performance indicators may also be used by an organisation to assist in assessing the effectiveness of their safety management procedures. Suitably selected indicators will enable the organisation to be proactive, as well as reactive, to safety issues. The auditor may examine the indicators selected, the resulting data and the organisation's actions when an adverse safety trend is identified.

6.2 Typical performance indicators are based upon the number of accidents, incidents and reportable occurrences. These are relatively rare events, however, and are only likely to indicate coarse trends in performance. Organisations should develop other measures of safety which relate to their particular operation and which will identify early trends in safety performance.

6.3 The auditor may use the results of past audits, and the efficiency and willingness of an organisation to respond to safety issues, as a performance indicator.

7 The Audit Team

7.1 It is important that those chosen to undertake any audit or safety inspection are suitably qualified and trained. The composition and number of those on the audit/inspection team will vary depending upon the size and complexity of the audit scope but it is important to ensure that there is sufficient expertise in specialist areas to ensure the validity of the audit.

7.2 In some cases it may be necessary to enlist the help of specialists; such specialists should be made aware of the audit objectives and their responsibilities. Ideally, a specialist should be involved at all stages of an audit (from planning to reporting).

7.3 Where more than one auditor is involved, a lead auditor, who will co-ordinate the individual auditor's activities, should be nominated.

8 The Audit Process

8.1 Audit Preparation

8.1.1 Thorough preparation is essential for a successful audit. It is important that the objectives and scope of the programme are identified and that the organisation is able to make appropriate staff available.

8.1.2 The facilities required by the auditor should be identified and the organisation made aware of these needs.

8.1.3 In order to assist in the pre-audit planning, the organisation may be asked to provide information relating to safety issues that the auditor will examine.

8.2 **Audit Timing.** The auditor will usually carry out routine audits by pre-arrangement with the organisation as part of the overall regulatory monitoring function. The safety regulatory auditor may also make an ad-hoc visit to the organisation although this course is only likely to be followed where there is evidence that the organisation may not be meeting the appropriate safety requirements.

8.3 **Inspection.** Some elements of an audit can only be fulfilled by inspection, typically the 'end result' needs to be evaluated against the expected result. It is important to remember that the audit is evaluating the system or process as a whole and that the objective of a safety management system is not simply to 'put a tick in each box' of a checklist at the time of the audit. The auditor will seek to confirm that organisation has procedures in place that should produce this result at all times and is able to identify any occasions when the system has failed.

8.4 **Management of change.** The organisation must have a system in place to ensure that changes to it's operation do not adversely effect safety. The system must ensure that, when appropriate, the Safety Regulator is informed of the changes and that the organisation has considered all of the implications of their implementation. This usually takes the form of a Safety Assurance Document. The auditor may examine the documentation associated with changes that have already been implemented and any those which are in preparation.

9 Audit Reporting and Follow-up actions

9.1 **Issue of reports.** Following the audit, a report detailing the findings will be compiled by the lead auditor. The organisation's representative responsible for safety should have the opportunity to comment on the report contents.

9.2 **Report findings**

9.2.1 The level of detail in the report may vary from a simple list of non-compliances found to a detailed description of areas of concern to the auditor and specific remedial recommendations. Where a specific non-compliance is identified, a reference to the relevant requirement should be included.

9.2.2 If remedial actions are agreed between the auditor and the organisation at the time of the audit, these should be documented.

9.2.3 In exceptional circumstances, where a safety regulatory auditor has found discrepancies or non-compliance which are serious enough to require the withdrawal or variation of a licence or approval, these findings will be described in the report. In such a case, these issues will be subject to further discussion between the auditor, senior SRG management and the organisation.

9.3 **Follow up actions**

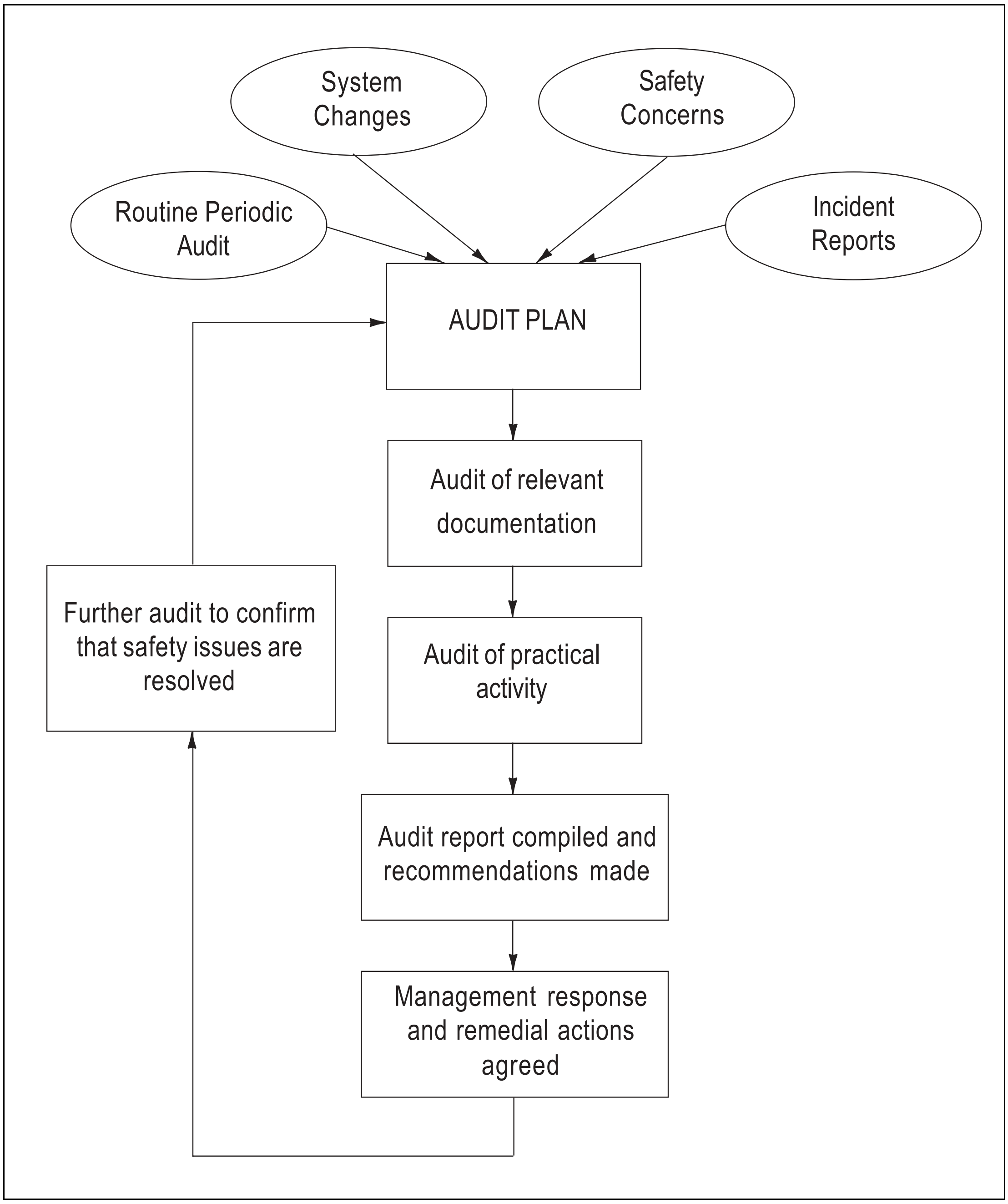
9.3.1 Where agreed rectification or remedial actions are noted the auditor will agree a timescale for completion with the organisation. It is the responsibility of the organisation to confirm, to the auditor, satisfactory completion of the agreed actions. If it is not possible for the actions to be completed within the agreed timescale for some reason, the auditor will require an acceptable alternative plan to be proposed by the organisation.

9.3.2 It should be noted that extensions to timescales for remedial actions will be granted as the exception rather than the rule. If no acceptable alternative can be proposed the auditor may direct the organisation to take specific actions to reduce the risk at issue.

9.3.3 The auditor may schedule a follow-up visit following the original audit in order to examine results or progress of the agreed remedial actions.

10 Generic Audit Process

The following flowchart illustrates the generic safety audit process. It should be noted that regulatory audits such as those carried out by SRG may require specific remedial action to be taken within a particular timescale.


System Changes
Safety Concerns
Routine Periodic Audit
Incident Reports
AUDIT PLAN
Audit of relevant documentation
Audit of practical activity
Audit report compiled and recommendations made
Management response and remedial actions agreed
Further audit to confirm that safety issues are resolved