Safety Case Evaluation

May 2019

This paper was prepared by the Safety Management International Collaboration Group (SM ICG). The purpose of the SM ICG is to promote a common understanding of Safety Management System (SMS)/State Safety Program (SSP) principles and requirements, facilitating their application across the international aviation community. In this document, the term “organization” refers to a product or service provider, operator, business, and company, as well as aviation industry organizations; and the term “authority” refers to the regulator authority, Civil Aviation Authority (CAA), National Aviation Authority (NAA), and any other relevant government agency or entity with oversight responsibility.

The current core membership of the SM ICG includes the Aviation Safety and Security Agency (AESA) of Spain, the National Civil Aviation Agency (ANAC) of Brazil, the Civil Aviation Authority of the Netherlands (CAA NL), the Civil Aviation Authority of New Zealand (CAA NZ), the Civil Aviation Authority of Singapore (CAAS), Civil Aviation Department of Hong Kong (CAD HK), the Civil Aviation Safety Authority (CASA) of Australia, the Direction Générale de l'Aviation Civile (DGAC) in France, the Ente Nazionale per l'Aviazione Civile (ENAC) in Italy, the European Aviation Safety Agency (EASA), the Federal Office of Civil Aviation (FOCA) of Switzerland, the Finnish Transport Safety Agency (Trafi), the Irish Aviation Authority (IAA), Japan Civil Aviation Bureau (JCAB), the United States Federal Aviation Administration (FAA) Aviation Safety Organization, Transport Canada Civil Aviation (TCCA), United Arab Emirates General Civil Aviation Authority (UAE GCAA), and the Civil Aviation Authority of United Kingdom (UK CAA). Additionally, the International Civil Aviation Organization (ICAO) is an observer to this group.

Members of the SM ICG:

- Collaborate on common SMS/SSP topics of interest
- Share lessons learned
- Encourage the progression of a harmonized SMS/SSP
- Share products with the aviation community
- Collaborate with international organizations such as ICAO and civil aviation authorities that have implemented or are implementing SMS and SSP

For further information regarding the SM ICG please contact:

Claudio Trevisan
EASA
+49 221 89990 6019
claudio.trevisan@easa.europa.eu

Sean Borg
TCCA
(613) 990-5448
sean.borg@tc.gc.ca

Mark Liptak
FAA, Aviation Safety
(202) 510-8010
Mark.Liptak@faa.gov

Neverton Alves de Novais
ANAC
+55 61 3314 4606
Neverton.Novais@anac.gov.br

Ash McAlpine
CASA
+ 07 3144 7411
Ashley.Mcalpine@casa.gov.au

SM ICG products can be found on SKYbrary at: http://bit.ly/SMICG

To obtain an editable version of this document, contact smicg.share@gmail.com.

Introduction to using this guide

The International Civil Aviation Organization's (ICAO's) Annex 19 requires organizations to develop and maintain a process identifying changes which may affect the level of safety risk associated with their aviation products and services and identifying and managing the safety risks that may arise from those changes. This guide provides authorities with a framework to evaluate safety cases for such changes. It is intended to provide the Regulatory Authority with assurance that a valid assessment of the change has been performed and documented by the organization. This guide also provides a way to record the evaluation.

This change documentation may come under different titles depending on the organization and the regulatory requirements, but generally these may be called safety cases, safety risk assessments, or aeronautical studies. In this document, the term "safety case" has been chosen. A safety case is a structured argument supported by a body of evidence that provides a compelling, comprehensible, and valid case that a system is safe for a given application in a given environment.

The Regulatory Authority should strive to perform a complete evaluation of the organization's safety case; however, the Regulatory Authority may consider sampling based on the level of involvement by the Regulatory Authority. The extent of the sample depends on the judgement and regulatory obligations of the evaluating Regulatory Authority.

The Regulatory Authority should consider the subjectivity of the evaluation and may have the evaluation peer reviewed.

This guide includes a matrix to help determine the level of involvement by the Regulatory Authority in the safety case at the start of the evaluation process. This considers:

- The depth and complexity of the change, and
- Judgement of the organization's capability and competence in managing the change safely.

Note: The guidance provided in this document may also be used by the Regulatory Authority to evaluate the adequacy of the assessment of safety issues performed by the organization. Safety issues include concerns identified by the regulator or the organization. Examples include the carriage of lithium batteries, an increase in number of occurrences, etc.

Note: The term assessment *is used for the service provider and the term* evaluation *is used to refer to activities performed to the Regulatory Authority.*

Regulatory requirements

Regulatory Authorities may require a formal safety case to be submitted in certain instances such as change management or addressing specific safety issues. There may also be specific regulatory requirements on how a safety case or safety risk assessment is formally accepted on the basis of existing regulatory obligations. These should always be followed, and this guide supports that formal acceptance.

This guide should be used to record the Regulatory Authority's evaluation of a safety case in order to demonstrate that the safety case was appropriately evaluated by the Regulatory Authority.

The Regulatory Authority may use tracking systems available to them to document their evaluation of safety cases. A template has been included as an appendix to this document and may be used to track any issues raised with the submitted documentation.

Evaluation steps

The evaluation has six steps that should be followed:

1. Formal acceptability

Evaluate the acceptability and completeness of the safety case.

2. Change description

Review the submitted documentation to ensure that the change has been adequately described, including its context and impacts, both internal and external.

3. Hazard identification

Ensure that appropriate hazard identification has been carried out and the range of consequences has been identified and documented.

4. Risk assessment

Review and evaluate whether probability and severity classifications are appropriate, justified, and applied consistently.

5. Risk mitigation and acceptance

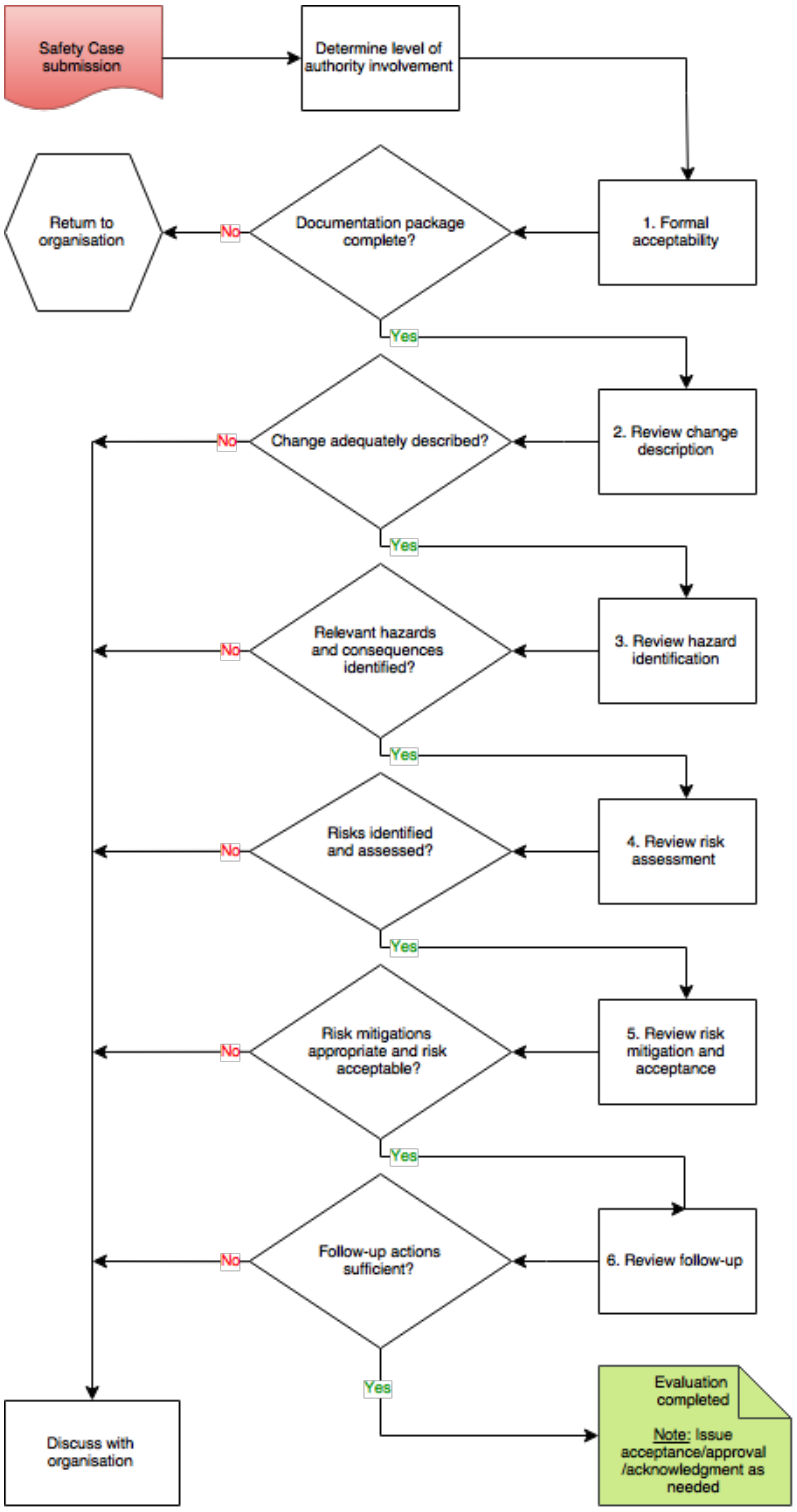
Evaluate the risk mitigations to determine whether actions are reasonable and robust and whether risk will be managed to an acceptable level.

6. Follow-up

Review how the organization plans to ensure that risk mitigations are effective and that the overall risk is effectively managed. Ensure that the organization periodically reviews the safety case.

Each step includes a series of actions to be taken by the Regulatory Authority's evaluator. For each action, there is guidance to assist the evaluator and a comments box to record what was sampled and any comments. As determined by the Regulatory Authority, the evaluator may not have to review each action but should indicate those that have been evaluated and those that haven't by recording "not evaluated" in the comments column.

Guide flowchart[1]



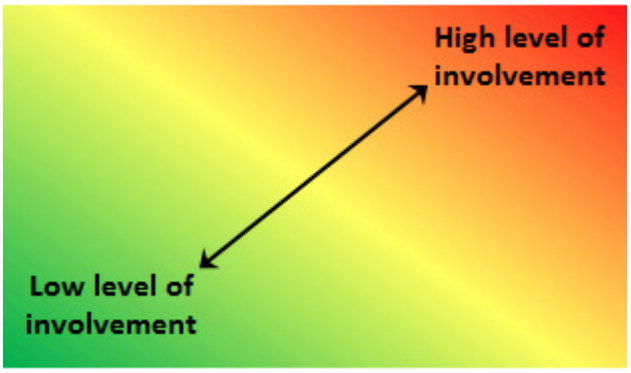
[1] In practice, the process may involve additional interaction and follow a different sequence based on the operational reality.

Safety case evaluation record

Organization:	**Title of change:**
Point of contact:	**Revision/issue no.**
Authority evaluators:	**Date received:**
Date documented:	

Determining the level of Regulatory Authority involvement

To determine the level of Regulatory Authority involvement in the safety case evaluation, the matrix below may be used (record the chosen level of involvement by marking the matrix). When determining the level of confidence of the Regulatory Authority, past oversight and the organization's capabilities should be considered. Complexity and scope of the change should be considered as part of the impact of the change. The further to the top-right of the matrix, the greater the level of involvement. Additionally, there may be little or no Regulatory Authority involvement necessary if the assessment is in the lower left corner of the matrix; however, consideration of regulatory obligations may still demand regulatory involvement. A low level of involvement could result in a greater use of sampling. In such a case, the approach to sampling should be identified and recorded.

What level of confidence does the Regulatory Authority have that the organization can successfully manage the proposed change?	**Low** **Medium** **High**	
		Low **Medium** **High**
		What is the impact of the change on the organization and the aviation system?

Level of Regulatory Authority involvement	Mark the matrix above	**Record justification:**
		Sampling approach used:
Is further regulatory involvement needed?	Yes	Proceed to Step 1.
	No	**Record justification:**

Safety case evaluation steps

Step 1 – Formal Acceptability		
Evaluate the acceptability and completeness of the safety case. *Note: If this step does not result in a positive evaluation, there is no need to complete the remaining steps. Return the safety case to the organization and indicate the changes required.*		
Instructions	**Evaluation Guidance**	**Comments**
1.1 Review the safety case to determine whether it meets the requirements and is sufficiently documented.	What type of change is being evaluated? - A proposal for an alternative means of compliance, a permission, exemption or approval. - Modifications to the type of operation or operational environment, etc. - Does it fulfil the regulatory requirements in terms of formal submission? - Appropriate person has signed off on the change. Does the safety case include the change description?	
1.2 Confirm that the safety case complies with the procedures of the organization.	The safety case should reflect the processes and procedures detailed in the organization's safety management documentation.	

Step 2 – Change Description		
Review the submitted documentation to ensure the change has been adequately described, including its context and impacts, both internal and external.		
Instructions	**Evaluation Guidance**	**Comments**
2.1 Review the documentation to determine whether it adequately describes the nature and scope of the change.	Who is making the change? What is being changed? Why is it being changed? How is it being changed?	
2.2 Determine whether there are similar changes assessed previously that could serve as a reference. *Note: Such similar changes would also serve as a reference for steps 3 to 6.*	Compare the following: - The data sources used; - The assumptions made in the previous safety cases as far as they are relevant; and - Information gleaned from previous related safety cases.	
2.3 Determine whether the change needs other Regulatory Authority departments or specialist involvement.	Where the change has a direct or indirect impact on another part of the aviation system, additional Regulatory Authority staff may need to be involved in the evaluation.	

Step 2 – Change Description		
Review the submitted documentation to ensure the change has been adequately described, including its context and impacts, both internal and external.		
Instructions	**Evaluation Guidance**	**Comments**
2.4 Review the documentation to determine whether the change description has considered all aspects of the organization/services.	As a result of the change, have some or all of the following aspects been considered? - People - Procedures - Equipment - Stakeholders - External/internal interfaces - Physical environment - Applicable rules - Impact on the safety culture[2] - Organizational structure	
2.5 Review the documentation to determine whether the direct and indirect impact of the change has been defined.	Does the defined impact go further than obvious ones? For example, indirect impacts on other operations/systems (e.g., for a change of taxiway layout, consider the impact on all users).	
2.6 Review the documentation to determine if the change being studied is not part of a broader change.	Does the documentation identify linkages to other potential changes affecting the same people or system? - The cumulative effects of the changes should be considered.	
2.7 Determine whether the change has an impact on compliance with standards and regulations.	Has the organization identified the regulations that are impacted by this change and has it ensured that it remains compliant?	

[2] For more information on safety culture, refer to the SM ICG Safety Culture pamphlet.

Step 3 – Hazard Identification		
Ensure that an appropriate hazard identification has been carried out and the range of consequences has been identified and documented. *Note: Depending on the level of involvement by the Regulatory Authority, the evaluation could be based on a sample of hazards.*		
Instructions	**Evaluation Guidance**	**Comments**
3.1 Determine who was involved in the process.	Determine whether the right people were selected (this may include subcontractors and external stakeholders). Have department/organizations identified as interfaces been involved in the hazard identification process?	
3.2. Confirm that the methods used to identify hazards and consequences are comprehensive.	Evaluate the methodology to confirm it adequately identifies hazards and related consequences. Determine whether identified hazards and consequences are appropriate. Consider if any hazards or consequences have been missed (ask an expert if needed). Review the suitability of data used.	
3.3 Confirm whether human performance-related hazards and their consequences have been identified.	The following may be considered: - Competency - Fatigue - Working environment - Communication - Human physiology - Human to machine interface - Stress - Error tolerance	

Step 3 – Hazard Identification		
Ensure that an appropriate hazard identification has been carried out and the range of consequences has been identified and documented. *Note: Depending on the level of involvement by the Regulatory Authority, the evaluation could be based on a sample of hazards.*		
Instructions	**Evaluation Guidance**	**Comments**
3.4 Determine whether hazards associated with interfaces have been considered.	Ensure that hazards related to internal interfaces between departments have been considered. Ensure that hazards related to external interfaces with organizations have been considered.	
3.5 Determine whether hazards associated with the transitional phase have been considered.	Ensure that hazards that may arise during the implementation of the change have been considered.	

Step 4 – Risk Assessment		
Review and evaluate whether probability and severity classifications are appropriate, justified, and applied consistently.		
Instructions	**Evaluation Guidance**	**Comments**
4.1 Determine whether probability, severity, and acceptability have been defined and used appropriately.	Are the classifications the same as those used in the organization's SMS? They may be qualitative definitions supported by expert judgement or quantitative definitions when data is available.	
4.2 Determine whether the probability and severity of each consequence has been recorded and the level of risk assessed.	Were probability, severity, and risk assessed before mitigating action was identified? Consider if the probability and severity identified are appropriate.	
4.3 Determine whether probability and severity have taken into account the impact of the change on existing risk controls.	Have impacts on existing risk controls been identified and considered as part of the risk assessment?	

Step 5 – Risk Mitigation and Acceptance		
Evaluate risk mitigations to determine whether actions are reasonable and robust and whether risk will be managed to an acceptable level.		
Instructions	**Evaluation Guidance**	**Comments**
5.1 Determine whether the acceptability of the risk has been assessed.	Has the level of risk been reviewed and risk acceptability determined? If the level of risk is acceptable, then additional risk mitigations will not be required.	
5.2 Determine whether appropriate risk mitigations have been identified and residual risk considered. *Note: Some hazards will have more than one mitigation.*	Have appropriate risk mitigations been identified? Are the mitigations reasonable and robust? Will risk mitigations continue to remain effective in the long term? Has the residual risk been calculated after taking into consideration all risk mitigations?	
5.3 Determine whether the risk mitigations have created any new risks or affected existing risk mitigations.	Do the identified risk mitigations impact any other activities or requirements directly or indirectly?	
5.4 Determine whether human factors principles have been considered in the choice of risk mitigation.	The following may be considered: - Workload - Competency and training requirements - Error tolerance - Communication requirements - Working environment - Psychosocial impact of the change - Human machine interface Is there an over reliance on human action as a risk mitigation?	

Step 5 – Risk Mitigation and Acceptance		
Evaluate risk mitigations to determine whether actions are reasonable and robust and whether risk will be managed to an acceptable level.		
Instructions	**Evaluation Guidance**	**Comments**
5.5 Determine whether the risk is adequately controlled and monitored or whether the justification for the risk acceptance is recorded.	Where a risk remains tolerable, has the decision to accept a risk been made by an appropriately authorized person? Has the rationale behind the acceptance been recorded?	

Step 6 – Follow-up		
Review how the organization plans to verify that risk mitigations are effective and that the overall risk is effectively managed. Ensure that the organization periodically reviews the safety case.		
Instructions	**Evaluation guidance**	**Comments**
6.1 Determine whether conclusions for the safety case have been included.	Review the conclusions. Ensure that the conclusion states that the change, including any needed transitional arrangements, can be implemented safely.	
6.2 Determine whether the organization ensures that all risk mitigations are implemented before the change takes place.	Has a person/organization been identified to ensure that risk mitigations will be implemented within the defined timescales?	
6.3 Determine whether the organization intends to verify that the risk mitigations are effective.	Does the organization have an appropriate plan to verify that the risk mitigations are effective? Have performance indicators been established? Are there adequate alternate plans in place?	
6.4 Determine whether the organization intends to ensure that assumptions in the safety case continue to be valid.	How will the organization monitor and review the assumptions after the change has taken place? Has the organization identified data needs to support validation of the assumptions?	
6.5 Determine when the safety case will be reviewed and how frequently.	Does the organization plan to review the safety case and re-assess the risks to ensure that the level of risk remains acceptable?	

Appendix 1

Summary observation form

Summary Observation Form		
Safety case:	**Evaluators:**	**Date:**
Evidence reviewed:		

Sample tracking form

Date raised	Evaluator	Type of observation	Observation and evidence	Update/closure rationale	Date closed