Safety Risk Management Methodologies (SRM)

ISO 31000 Risk management - guidelines

This document was developed by the Safety Management Panel (SMP). It is intended to support safety experts in the application of risk management methodologies. Any comments to this material should be forwarded to safetymanagement@icao.int.

Version 0.4 – June 2022

TABLE OF CONTENTS

1. DESCRIPTION

1.1 Purpose of the methodology

International Standard ISO[1] *31000 Second edition 2018-02 Risk management - Guidelines* (*ISO 31000*) provides a common, global guideline on the management of any type of risk faced by any organization[2] regardless of industry or sector. *ISO 31000* encourages the published guidelines to be customized as required for each organization and in this manner can be applied to any activity including decision making at all levels.

ISO 31000 is supported by *ISO Guide 73:2009 Risk management — Vocabulary (ISO Guide 73:2009)* which defines the basic risk management vocabulary to develop a common understanding on risk management concepts and terms among organizations and functions, and across different applications and types.

International Standard *IEC*[3] *31010 Edition 2.0 2019-06 Risk management – Risk assessment techniques (IEC 31010*) provides guidance on the selection and application of various techniques that can be used to help improve how uncertainty is considered and to help understand risk. The techniques are used in support of the *ISO 31000* risk management process, within the risk assessment steps of identifying, analyzing and evaluating risk, and more generally whenever there is a need to understand uncertainty and its effects. While *IEC 31010* is primarily intended for the electrical and electronic fields, the standard was developed in in cooperation with ISO and many of the identified techniques are considered useful across other industries and sectors.

1.2 Theoretical basis (Model)

ISO 31000 details a risk management framework and risk management process to support the assessment and management of risk.

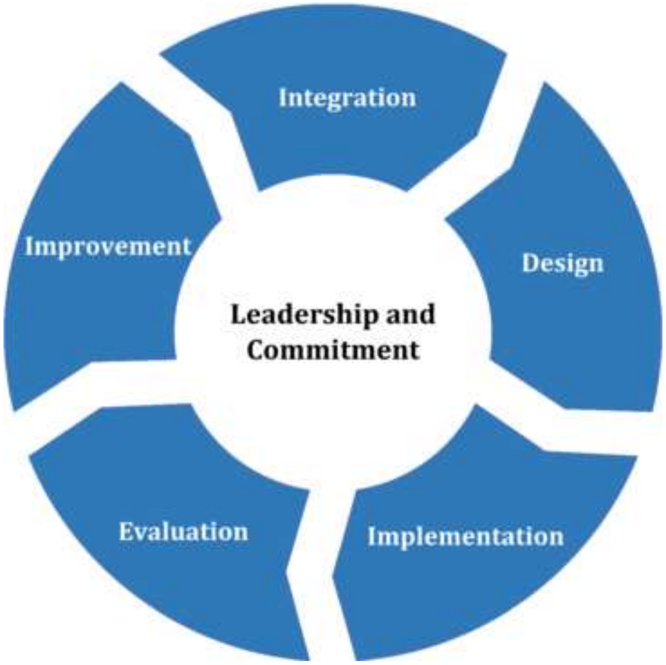
The risk management framework detailed in *ISO 31000* assists the organization to integrate risk management into significant activities and functions including decision making. Integration of the risk management framework into an organization requires significant stakeholder support, particularly from senior management. The ISO 31000 framework is detailed in Figure 1.

[1] ISO (the International Organisations for Standardization) is a worldwide federation of national standard bodies (ISO member bodies).

[2] For the purposes of this document, an ‘organization’ can be taken to mean either a servicer provider or a National Aviation Authority (State).

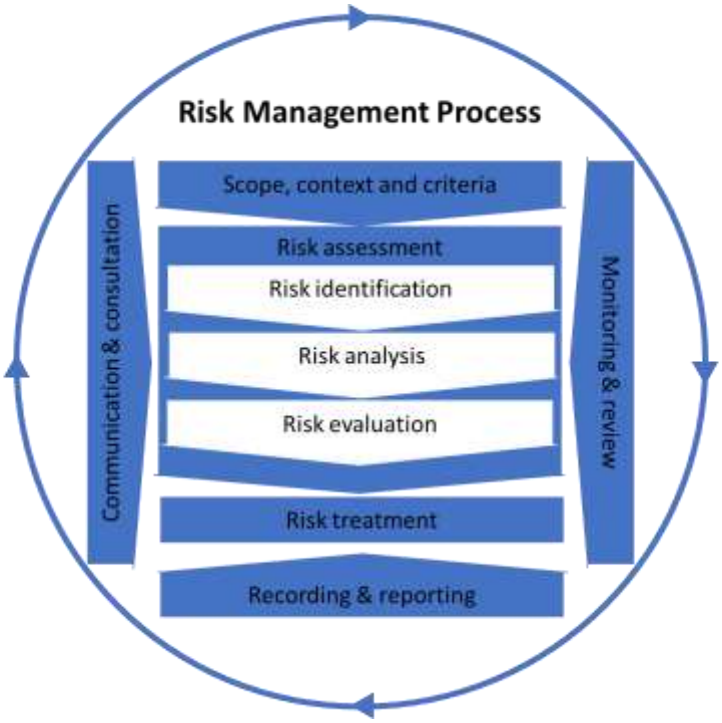
[3] The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields.

Figure 1 - ISO 31000 Risk Management Framework



The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. The process is illustrated in Figure 2.

Figure 2 - ISO 31000 Risk Management Process



1.3 Risk acceptance method and criteria (where applicable)

The *ISO 31000* risk management process requires organizations to establish the amount and type of risk that may or may not be taken to guide the development of risk criteria and includes a risk evaluation stage to support decisions around risk acceptance. Risk evaluation typically involves comparing the results of the risk analysis stage against an established criteria (pre-defined risk tolerance levels) to determine what further action (if any) is required.

The *ISO 31000* risk evaluation stage provides guidelines for what actions can be taken but provides no further details or explanation on how to establish risk criteria. Guidelines for the implementation of the decision options identified in risk evaluation are included in the risk treatment stage of *ISO 31000*.

The *ISO 31000* risk evaluation stage is loosely consistent with intent of the example methodology provided in Section 2.5.5 (Safety risk tolerability) of *ICAO Doc 9859 (4th Edition)*. In this methodology safety risk tolerability is determined by comparing the assessed safety risk index rating against pre-defined safety risk tolerability criteria to determine if a risk is acceptable, tolerable or intolerable.

1.4 Key terms and definitions (e.g. hazard/threat, likelihood/probability, severity)

Table 1 - ISO 31000 key terms and definitions

Term	ISO 31000 Definition*
Hazard	Source of potential harm
Risk	Effect of uncertainty on objectives
Level of risk	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood
Event	Occurrence or change of a particular set of circumstances ****Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".* *Note 4 to entry: An event without consequences (3.6.1.3) can also be referred to as a "near miss", "incident", "near hit" or "close call"****
Likelihood	Chance of something happening
Consequence	Outcome of an event (3.5.1.3) affecting objectives
Risk treatment	Process to modify risk ****Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction"****
Control	Measure that is modifying risk

** Only pertinent notes from ISO 31000 have been included.*

Note – A comparison of terms and definitions in ISO 31000 and ICAO Doc 9859 is included in Table 2.

1.5 Data/Information Inputs

Data is required to evaluate uncertainty and consequently to evaluate risks for this reason ensuring access to relevant data is an important aspect of any risk assessment.

ISO 31000 advocates for establishing the internal and external context of the risk within the broader organization as part of the risk management process. *ISO 31000* further acknowledges that the risk assessment process may be influenced by a divergence of opinions, biases, perceptions of risk and judgements. Other influences can include the quality of the information used, the assumptions and exclusions made, any limitation of the techniques and how they are executed.

ISO 31000 acknowledges that highly uncertain events are difficult to quantify which can be an issue when analyzing events with severe consequence (such of those often considered in aviation safety risk assessments). For this reason, *ISO 31000* suggests using a combination of risk analysis techniques to provide greater insight. This is consistent with *ICAO Doc 9859* '*safety risk assessments sometimes have to use qualitative information (expert judgement) rather than quantitative data due to the unavailability of data'*.

1.6 Tools available (where applicable)

While *ISO 31000* provides no tools for the management of risks, due to the wide global acceptance of the *ISO 31000* methodology there are numerous off the shelf risk management software products available that are based on the *ISO 31000* process.

IEC31010 Risk management – Risk assessment techniques (Table A.2) provides techniques for identifying, analyzing and evaluating risks, which helps the users in a better implementation of *ISO 31000*.

2. USER FACTORS

2.1 Applications (e.g. general or sector-specific)

ISO 31000 provides a common, global guideline on the management of risk faced by any organization regardless of industry or sector and therefore, while not being a specific aviation risk process can be adopted by any aviation sector. *ISO 31000* encourages the published guidelines to be customized as required to each organization and therefore can be successfully applied to aviation at a Service Provider or State level.

2.2 Users (e.g. general workforce, management, safety analysts, trainers)

ISO 31000 is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance. *ISO 31000* advocates that everyone in an organization has responsibility for managing risk. Typically, a customized *ISO 31000* methodology would be incorporated into an organizations risk management procedure and then all staff responsible for assessing, managing or owning risk would follow the defined procedures.

2.3 Evaluation of Complexity

ISO 31000 is a high-level framework and process that is designed to be applied across a broad range of industries and activities. As such ISO 31000 is not considered complex and there is no specific training or software required to implement the concepts included in *ISO 31000*. *ISO 31000* can be readily adopted in most organizations though a dynamic and iterative process provided there is the appropriate leadership commitment from management.

Complexity may arise attempting to apply the broad concept included in *ISO 31000* to specific aviation operational activities. This is where considering *ISO 31000* in conjunction with the guidance included in *ICAO Doc 9859* can be useful in providing guidance on the practical aviation application of ISO 31000 concepts and reduce any associated complexity.

2.4 Availability of training

As an international standard applied across a broad range of industries training to *ISO 31000* is readily available through a range of providers worldwide (States and organizations are encouraged to refer to their national standardization body for details on available training options). Training on applying *ISO 31000* concepts specifically to aviation related activities is less available.

Little to no training was identified that combines *ISO 31000* concepts with the guidance advocated for by ICAO and included in *ICAO Doc 9859.*

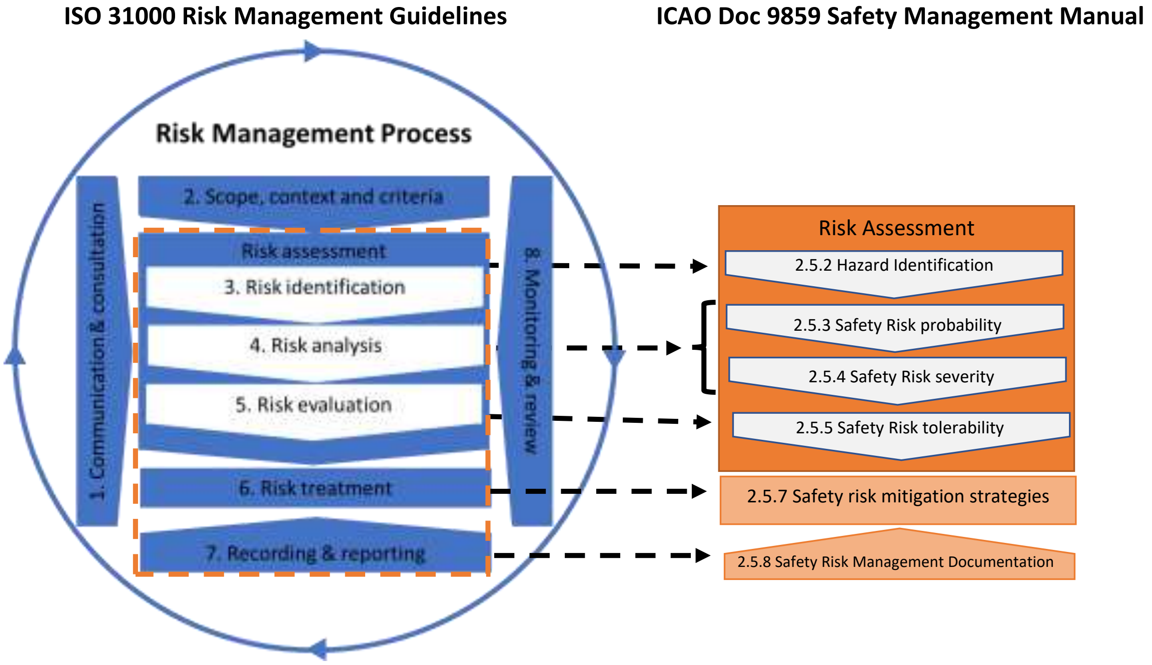
3. QUALITY AND CONSISTENCY

3.1 Consistency/Differences from SMM Concepts, Terms and Definitions (e.g. flow from, hazard/source of risk, to: immediate outcome and ultimate consequence)

Often *ISO 31000* and *ICAO Doc 9859* are seen as different and inconsistent approaches to risk management. Whilst there are numerous differences in terms of the terminology and the overall focus of the methodology the two approaches should not be considered inconsistent but instead are compatible and in fact complimentary.

ISO 31000 provides guidelines for a wholistic *Risk Management Process* and is not just a risk assessment methodology. The *ISO 31000* methodology considers more than just the assessment of the risk and includes additional standards around communication and consultation, scope, context, criteria, recording and reporting and monitoring and review. Guidance contained in *ICAO Doc 9859* is more focused around the risk assessment process and the *ISO 31000* risk identification, risk analysis and risk evaluation steps. The *ICAO Doc 9859* safety risk management guidelines can be considered a subset of and complementary to the risk management process included in *ISO 31000* as depicted in Figure 3.

Figure 3 - ISO 31000 Risk Management Process versus ICAO Doc 9859 (4th Edition) Safety Risk Management Guidelines


ISO 31000 Risk Management Guidelines
ICAO Doc 9859 Safety Management Manual
Risk Management Process
1. Communication & consultation
2. Scope, context and criteria
Risk assessment
3. Risk identification
4. Risk analysis
5. Risk evaluation
6. Risk treatment
7. Recording & reporting
8. Monitoring & review
Risk Assessment
2.5.2 Hazard Identification
2.5.3 Safety Risk probability
2.5.4 Safety Risk severity
2.5.5 Safety Risk tolerability
2.5.7 Safety risk mitigation strategies
2.5.8 Safety Risk Management Documentation

Due to *ISO 31000* being a common approach to managing any type of risk and not being industry or sector specific the guidelines are very high level and include general considerations only, with no specifics on how to complete each step of the process. It is typically left to each organization to tailor the *ISO 31000* guidance to their specific context.

In order to improve the specific guidance around risk assessments, *IEC31010 Risk management – Risk assessment techniques*, has been published which details suggested techniques for use within the risk assessment steps of identifying, analysing and evaluating risk as described in *ISO 31000*, and more generally whenever there is a need to understand uncertainty and its effects.

The guidance on completing an aviation safety risk assessment included in ICAO Doc 9859 is compatible with the *ISO 31000* risk management process. The ICAO Safety risk severity / probability /tolerability guidance is mostly consistent with the consequence/likelihood matrix technique described in IEC31010 (Section B.10.3). *ISO 31000* specifically requires organizations to customize the risk management process to suit their activities and the broader context. Applying the ICAO 9859 process for risk assessments to the *ISO 31000* methodology would be considered as an initial customization. ICAO Doc 9859 also advocates for organizations to customize their safety risk management procedures to ensure they are suitable for the organization, which remains broadly consistent with *ISO 31000* guidelines.

Risk Analysis

The risk analysis stage is where the nature and characteristics of the risk are determined, including the level of risk. *ISO 31000* does not mandate a particular method to measure the level of risk, instead *IEC 31010* provides guidance on measuring the level of risk through either qualitative, semi-quantitative or quantitative approaches.

ICAO Doc 9859 overarching purpose is to support States in meeting their obligations, particularly for the management of aviation safety risk. Based on this *ICAO Doc 9859* includes an example safety risk matrix (ICAO Doc 9859 Table 3) with supporting examples of safety risk probability (ICAO Doc 9859 Table 1) and safety risk severity descriptors (ICAO Doc 9859 Table 2). This example is used to measure the safety risk (level of risk in *ISO 31000* terms) and would be considered qualitative approach under the *IEC 31010 guidance*. Inclusion of quantitative descriptors in the safety risk probability table (ICAO Doc 9859 Table 1) would be a semi-quantitative approach.

Whilst compatible, *ISO 31000* and ICAO Doc 9859 do differ in the definitions of key terminology. Whilst not significant enough to make the two guidelines incompatible, the difference in terminology can cause confusion when being applied operationally. Table 2 details the key risk management definitions in *ISO 31000* compared to those included in *ICAO Doc 9859*.

Table 2 - Comparison of ISO 31000 compared to ICAO Doc 9859 Definitions

Term	ISO 31000 Definition	ICAO 9859 Definition	Comments
Hazard	Source of potential harm	A condition or object with the potential to cause or contribute to an aircraft incident or accident	The 'harm' in ISO31000 is the aircraft incident or accident as defined in the ICAO Doc 9859.
Risk	effect of uncertainty on objectives		
Safety Risk		The predicted probability and severity of the consequences or outcomes of a hazard.	ICAO Doc 9859 definition more closely aligned to *'Level of Risk'* definition in ISO 31000.
Level of risk	magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood		Similar to ICAO *'Safety Risk'* definition
Event	occurrence or change of a particular set of circumstances *Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".* *Note 4 to entry: An event without consequences (3.6.1.3) can also be referred to as a "near miss", "incident", "near hit" or "close call".*		Could be described as a realized hazard (before we get the consequence) in ICAO Doc 9859 terms. Ie. *Contaminated runway* (hazard) causes a *runway excursion* (event) resulting in *damage / lives lost* (consequence).
Likelihood	chance of something happening		
Safety Risk Probability		The likelihood that a safety consequence or outcome will occur.	
Consequence	outcome of an event (3.5.1.3) affecting objectives	An outcome that can be triggered by a hazard	
Severity		The extent of harm that might reasonably be expected to occur as a consequence or outcome of the identified hazard	
Risk treatment	process to modify risk *Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk*		Similar intent to risk mitigation.

	elimination", "risk prevention" and "risk reduction".		
Risk Mitigation		The process of incorporating defenses, preventive controls or recovery measures to lower the severity and/or likelihood of a hazard's projected consequence.	Similar intent to risk treatment.
Control	measure that is modifying risk		Similar intent to defenses.
Defenses		Specific mitigating actions, preventive controls or recovery measures put in place to prevent the realization of a hazard or its escalation into an undesirable consequence.	Similar intent to control.

3.2 Validity and reliability of outputs

ISO 31000 is a high-level framework and process that is designed to be applied across a broad range of industries and activities and that is required to be customized to an organizations activity to be effective. Noting the high-level nature of the guidelines the effectiveness of implementation and therefore the validity and reliability of the outputs can vary based on how the framework and guidelines are implemented within an organization.

3.3 Overall pros and cons (i.e. strengths and limitations)

Pros	Cons
• Standard high-level process that can be applied across any industry. • Globally recognized standard. • Broad international consensus on suitability of methodology. • Significant training available across all regions. • Applies to more than just aviation safety – organisations can use a standard underpinning methodology to consider all types of organisational risk	• Light on detail – a high level document that focused on considerations for process and frameworks. Does not provide meaningful detail on how to implement (although *IEC 31010* gives good options and examples for practical implementation). • Not specific to aviation • Terminology differs from ICAO Doc 9859 – terminology difference can too often derail the effective implementation of process and procedure.

3.4 Team assessment of usability

ISO 31000 is considered a straightforward standard that can be easily adopted for aviation organizations. Organizations seeking to implement an *ISO 31000* based process for aviation activities should consider how

ISO 31000 and ICAO Doc 9859 guidance differs and how when considered together the two methodologies can complement each other and result in improved risk outcomes.

4. ADDITIONAL INFORMATION

4.1 Abbreviations

Abbreviations	Meaning	Notes
IEC	International Electrotechnical Commission	
ISO	International Standards Organisation	
SRM	Safety Risk Management	
SRA	Safety Risk Assessment	
SMM	Safety Management Manual	ICAO document 9859

4.2 Literature - reference

- Safety Management Manual (Doc 9859) 4th Edition, International Civil Aviation Organization, Montreal, 2018
- International Standard ISO 31000 2nd Edition, Risk Management Guidelines, International Standards Organisation, Geneva, 2018
- International Standard IEC 31010, Risk Management – Risk Assessment Techniques, International Electrotechnical Commission, Geneva, 2019