IS-BAO 20th Edition

Guidance - FAA SMSVP

November 01st, 2022

International Business Aviation Council (IBAC)
Suite 16.33, 999 Robert-Bourassa Boulevard
Montreal, Quebec, H3C 5J9, Canada
Tel: 1-514-954-8054 Fax: 1-514-954-6161
www.ibac.org

**IS-BAO (An International Standard for
Business Aircraft Operations) Guidance**

Table of Contents

THIS PAGE
INTENTIONALLY
LEFT BLANK

Introduction

Applicability

This chapter of the Guidance material does not expand on any IS-BAO Standard or Recommended Practice. Instead, it assists US operators that seek or wish to maintain FAA acceptance of their SMS under the FAA Safety Management System Voluntary Program (SMSVP) in FAA Order 8900.1, Volume 17, Chapter 3, by providing guidelines to assess, monitor, and manage their compliance with the SMSVP. In other words, this document supplements other IS-BAO Guidance material without replacing any of it.

Document structure

This chapter follows the SMSVP Standard (Figure 17-3-3A) from Subpart B to F.

Contents

Excerpts from the SMSVP are provided when conformance with the IS-BAO Standard does not readily provide a comparable level of compliance with the SMSVP Standard. These excerpts contain the number and title of the section, as well as the associated SMSVP Standard(s). Whenever conformance with IS-BAO is perceived as sufficient to comply with SMSVP, only the title of the SMSVP section is provided for reference.

In the excerpts, the color blue is used solely to identify specific portions of the SMSVP Standard where conformance with IS-BAO does not necessarily equate to compliance with the SMSVP. In such case, the operator must supplement its existing policies, processes, and/or procedures to appropriately meet the SMSVP Standard. Any other portion (i.e., in black) of an excerpt of the SMSVP Standard can be considered as met and compliant when conforming with IS-BAO.

Note: Where the SMSVP refers to certificate holder, the term has been replaced by [operator] in this document.

Revision Original
November 01, 2022

3

**THIS PAGE
INTENTIONALLY
LEFT BLANK**

Guidance

5.21 Safety Policy

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.23 Safety Accountability and Authority

(a) The [operator] must define accountability for safety within the organization's safety policy for the following individuals:
    (1) Accountable executive, as described in 5.25.
    (2) All members of management in regard to developing, implementing, and maintaining SMS processes within their area of responsibility, including, but not limited to:
        (i) Hazard identification and safety risk assessment.
        (ii) Assuring the effectiveness of safety risk controls.
        (iii) Promoting safety as required in subpart E of this Standard.
        (iv) Advising the accountable executive on the performance of the SMS and on any need for improvement.
    (3) Employees relative to the [operator]'s safety performance.
(b) The [operator] must identify the levels of management with the authority to make decisions regarding safety risk acceptance.

IBAC guidance:

IS-BAO 3.1.2.1 requires operators to document and communicate safety responsibilities, accountability and authorities throughout the organization. However, IS-BAO does not require reference to such responsibilities, accountability and authorities to be made within the safety policy, and as such operators must review their safety policy to ensure it includes those items or references the section of their manual / documentation where such responsibilities, accountability and authorities are documented.

Additionally, IS-BAO does not specifically address the items listed in 5.23(a)(2). Therefore, operators need to review and/or document safety accountabilities to ensure alignment with the SMSVP, particularly those of any manager. When doing so, operators could consider first defining baseline safety accountabilities that are common to all staff members, then detail 'add-on' safety accountabilities for each relevant managerial position, to include the minimum items listed in 5.23(a)(2)(i) through 5.23(a)(2)(iv).

5.25 Designation and Responsibilities of Required Safety Management Personnel

(a) Designation of the accountable executive. The [operator] must identify an accountable executive who, irrespective of other functions, satisfies the following:
    (1) Is the final authority over operations authorized to be conducted under the [operator]'s certificate(s).

(2) Controls the financial resources required for the operations to be conducted under the [operator]'s certificate(s).

(3) Controls the human resources required for the operations authorized to be conducted under the [operator]'s certificate(s).

(4) Retains ultimate responsibility for the safety performance of the operations conducted under the [operator]'s certificate.

(b) Responsibilities of the accountable executive. The accountable executive must accomplish the following:

(1) Ensure that the SMS is properly implemented and performing in all areas of the [operator]'s organization.

(2) Develop and sign the safety policy of the [operator].

(3) Communicate the safety policy throughout the [operator]'s organization.

(4) Regularly review the [operator]'s safety policy to ensure it remains relevant and appropriate to the [operator].

(5) Regularly review the safety performance of the [operator]'s organization and direct actions necessary to address substandard safety performance in accordance with 5.75.

(c) Designation of management personnel. The accountable executive must designate sufficient management personnel who, on behalf of the accountable executive, are responsible for the following:

(1) Coordinate implementation, maintenance, and integration of the SMS throughout the [operator]'s organization.

(2) Facilitate hazard identification and safety risk analysis.

(3) Monitor the effectiveness of safety risk controls.

(4) Ensure safety promotion throughout the [operator]'s organization as required in subpart E of this Standard.

(5) Regularly report to the accountable executive on the performance of the SMS and on any need for improvement.

IBAC guidance:

IS-BAO 3.1.2.1 requires the operator to identify the Accountable Executive who has ultimate accountability for the safety performance of the organization. Operators must make sure that the person they have identified as their AE, apart from retaining ultimate accountability for safety performance, also satisfies the 3 other aspects listed in 5.25(a); namely, that the AE:

– Is the final authority over operations authorized to be conducted under the operator's certificate(s);

– Controls the financial resources required for the operations to be conducted under the operator's certificate(s); and

– Controls the human resources required for the operations authorized to be conducted under the operator's certificate(s).

Additionally, IS-BAO does not specifically address the items listed in 5.25(b)(4) and (5), and 5.25(c). Therefore, operators need to:

– Review and/or document the duties and accountabilities of their Accountable

Executive to ensure alignment with the SMSVP. Particular attention must be paid to documenting that the AE:
- o Has control over both human and financial resources required to operate safely,
- o Designates sufficient management personnel,
- o Regularly reviews the operator's Safety Policy to ensure it remains relevant and appropriate to the operator,
- o Regularly reviews the operator's safety performance, and
- o Directs any necessary action to address substandard safety performance.
- – Review and/or document management personnel's duties and responsibilities so as to ensure compliance with 5.25(c)(1) through (5).

5.27 Coordination of Emergency Response Planning

Where emergency response procedures are necessary, the [operator] must develop and the accountable executive must approve as part of the safety policy, an emergency response plan that addresses at least the following:
(a) Delegation of emergency authority throughout the [operator]'s organization;
(b) Assignment of employee responsibilities during the emergency; and
(c) Coordination of the [operator]'s emergency response plans with the emergency response plans of other organizations it must interface with during the provision of its services.

IBAC guidance:

Chapter 4 of the IS-BAO requires all registered operators to develop an Emergency Response Plan covering the contents listed in IS-BAO 4.1. Some adjustments may be needed to the operator's Emergency Response document(s) to ensure alignment with the SMSVP. If it's not already the case, the manual that contains the ERP must be formally approved by the Accountable Executive, and the operator's Safety Policy must refer to the AE's approval of the ERP.

In addition, operators need to ensure that the ERP address the aspects listed in 5.27(a) and 5.27(b), namely:
- – Delegation of emergency authority throughout the organization; and
- – Assignment of employee responsibilities during the emergency.

Duties and responsibilities of staff members involved in any response to an emergency should be documented as precisely as practical, and foresee the possibility of having to delegate some or all of a staff's emergency authority. The delegation process should assist in clearly identifying under whose authority certain tasks will then be performed, when and how the delegation starts and ends, and how the transfer of authority will be kept on record.

5.51 Applicability

A [operator] must apply safety risk management to the following:
(a) Implementation of new systems.
(b) Revision of existing systems.
(c) Development of operational procedures.
(d) Identification of hazards or ineffective risk controls through the safety assurance processes in subpart D of this Standard.

IBAC guidance:

IS-BAO 3.2.1 and 3.2.2 require operators to establish hazard identification and safety risk management processes. Hazards may be identified from the methods required by IS-BAO 3.2.1 (including but not limited to accident / incident investigation, voluntary and mandatory safety reporting, and review of external sources of safety information) or the various safety assurance / safety performance processes (internal audits and evaluations, safety performance monitoring and measurement, management of change and continuous improvement of the SMS). Collectively, these cover all the triggers for Safety Risk Management listed in 5.51, since:

- 5.51(a) through (c) constitute changes to the organization's systems, processes or operational procedures and, as such, should trigger an instance of the Management of Change process established by the organization to conform with IS-BAO 3.3.2, which feeds into the Safety Risk Management process required by IS-BAO 3.2.1 and 3.2.2,
- 5.51(d) refers to hazards or ineffective controls identified through the various Safety Assurance processes required by IS-BAO 3.3.1, 3.3.2 and 3.3.3, and which also feed into the Safety Risk Management process required by IS-BAO 3.2.1 and 3.2.2.

That said, IS-BAO requires operators to establish criteria to determine which types of changes (internal and external) require the use of the Management of Change process according to the impact on the organization's safety, and notes that these criteria should consider items such as operational changes, organizational changes and changes in key personnel. Although this covers the triggers listed in 5.51 (a) through (c), in order to ensure full alignment with the SMSVP, operators must ensure that their criteria to conform with IS-BAO 3.3.2 explicitly include the implementation of new systems, the revision of existing systems, and the development of operational procedures.

5.53 System Analysis and Hazard Identification

(a) When applying safety risk management, the [operator] must analyze the systems identified in 5.51. Those system analyses must be used to identify hazards under paragraph (c) of this section, and in developing and implementing risk controls related to the system under 5.55(c).
(b) In conducting the system analysis, the following information must be considered:
   (1) Function and purpose of the system.
   (2) The system's operating environment.
   (3) An outline of the system's processes and procedures.

(4)   The personnel, equipment, and facilities necessary for operation of the system.
(c) The [operator] must develop and maintain processes to identify hazards within the context of the system analysis.

IBAC guidance:

IS-BAO 3.2.1 and 3.2.2 require operators to establish hazard identification and safety risk management processes. Operators must establish methods to identify hazards, as required in IS-BAO 3.2.1, and also ensure hazards are identified from the various safety assurance / safety performance evaluation processes required by IS-BAO 3.3.

In order to appropriately identify hazards, it is key that the operator has a deep understanding of the activities they conduct, so that they do not miss hazards due to an incomplete view of what is needed to accomplish those tasks and the circumstances in which they will take place. IS-BAO recognizes that aspect, as discussed in Guidance for chapter 3.2, however there is no explicit associated requirement in the IS-BAO Standard for operators to analyse the system related to safety information leading to any hazard identification and safety risk management process.

This safety information may come from the methods required by IS-BAO 3.2.1 (including but not limited to accident / incident investigation, voluntary and mandatory safety reporting and review of external sources of safety information) or the various safety assurance / safety performance processes (internal audits and evaluations, safety performance monitoring and measurement, management of change and continuous improvement of the SMS). As discussed above in this document, collectively these cover all the systems addressed by 5.51, namely:

5.51 Applicability.
A [operator] must apply safety risk management to the following:
(a)   Implementation of new systems.
(b)   Revision of existing systems.
(c)   Development of operational procedures.
(d)   Identification of hazards or ineffective risk controls through the safety assurance processes in subpart D of this Standard.

Therefore, in order to ensure alignment with the SMSVP, operators must ensure that, when safety information triggering safety risk management is obtained from the sources referred to above, they first and foremost conduct the system analysis required by 5.53(a) and (b), making sure that in that process they consider the following aspects listed in 5.53(b)(i) through 5.53(b)(iv):
–   Function and purpose of the system.
–   The system's operating environment.
–   An outline of the system's processes and procedures.
–   The personnel, equipment, and facilities necessary for operation of the system

This system analysis must be used as the foundation for the identification of hazards, and the associated safety risk analysis, assessment and control processes established by the organization

in accordance with IS-BAO 3.2.2.

For the past seven decades, system analyses have come in many shapes and forms. Through trial and error, several approaches matured and spread in multiple industries (e.g., HAZOP, FMEA, Tree Analyses, BowTie, STPA/STAMP, etc.). However, some are more appropriate for flight operations than others, especially when it comes to addressing the human element in the system(s). Put simply, human performance varies. The challenge is therefore to analyze the operator's system(s) by finding the right balance between:

– An 'engineering approach' that may sometimes see humans as mere components that can -and should- be measured, controlled, and managed to constraint their performance and outputs within a certain predictable bandwidth, and

– A 'mindful but potentially satisficing and even *laissez-faire* approach' that may sometimes dismiss too quickly the benefits of system-thinking, proceduralization, and standardization.

Regardless of the size of the operation, there's benefit in applying system-thinking to first identify pertinent hazards (both inside and outside of the operation), then to prioritize and manage the associated risks considering the finite resources of the operator. Appendix 2 details the tenets of system-thinking that should underline and guide system analyses and risk assessments.

5.55 Safety Risk Assessment and Control

(a) The [operator] must develop and maintain processes to analyze safety risk associated with the hazards identified in 5.53(c).
(b) The [operator] must define a process for conducting risk assessment that allows for the determination of acceptable safety risk.
(c) The [operator] must develop and maintain processes to develop safety risk controls that are necessary as a result of the safety risk assessment process under paragraph (b) of this section.
(d) The [operator] must evaluate whether the risk will be acceptable with the proposed safety risk control applied, before the safety risk control is implemented.

IBAC guidance:

As discussed in the IS-BAO Guidance for section 3.2 of the IS-BAO Standard and in question 3.2.2.S2c of the IS-BAO protocols, IS-BAO registered operators are expected to reassess a safety risk in terms of its probability and severity post mitigation actions, to confirm that the risk has been brought to a tolerable level. To ensure alignment with the SMSVP, however, this must be accomplished before the safety risk control is implemented, as per 5.55(d). As such, operators need to assess the outcomes of their risk management process and ensure that the risk controls (i.e., mitigation) under consideration will lead to an acceptable residual risk before the risk controls are effectively implemented.

5.71 Safety Performance Monitoring and Measurement

(a) The [operator] must develop and maintain processes and systems to acquire data with respect to its operations, products, and services to monitor the safety performance of the organization. These processes and systems must include, at a minimum, the following:

(1) Monitoring of operational processes.
(2) Monitoring of the operational environment to detect changes.
(3) Auditing of operational processes and systems.
(4) Evaluations of the SMS and operational processes and systems.
(5) Investigations of incidents and accidents.
(6) Investigations of reports regarding potential noncompliance with regulatory standards or other safety risk controls established by the [operator] through the safety risk management process established in subpart C of this Standard.
(7) A confidential employee reporting system in which employees can report hazards, issues, concerns, occurrences, incidents, as well as propose solutions and safety improvements.

(b) The [operator] must develop and maintain processes that analyze the data acquired through the processes and systems identified under paragraph (a) of this section and any other relevant data with respect to its operations, products, and services.

IBAC guidance:

Although IS-BAO requires implementation of a safety reporting system as part of IS-BAO Standard 3.2.1 and also requires operators to implement a policy protecting any safety-related data (from all sources to include the safety reporting system) from inappropriate use, it does not specify that the safety reporting system must be confidential. Therefore, unless already clearly stated in their SMS manual/document and implemented, operators need to ensure that their reporting system strictly protects the confidentiality of reporters, from the initial submission of information to its storage. The guiding principle remains to maximize the ease of reporting while minimizing the anxiety of reporting. Clear policies, processes, and procedures are needed, as applicable, to comprehensively describe how reports are handled and protected, by whom, but also who doesn't have access to them and what uses are forbidden. When designing a report form or selecting an IT solution, operators are encouraged to give precedence to narratives rather than to a flurry of boxes to tick and values to report. Both are valuable and needed to lead further investigations, and therefore space for both must be foreseen. However, personal accounts should come first and also invite the reporter to share suggestions and systemic improvements.

5.73 Safety Performance Assessment

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.75 Continuous Improvement

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.91 Competencies and Training

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.93 Safety Communication

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.95 SMS Documentation

Conformance with IS-BAO is perceived as sufficient to comply with this section of the SMSVP.

5.97 SMS Records

(a)   The [operator] must maintain records of outputs of safety risk management processes as described in subpart C of this Standard. Such records must be retained for as long as the control remains relevant to the operation.
(b)   The [operator] must maintain records of outputs of safety assurance processes as described in subpart D of this Standard. Such records must be retained for a minimum of 5 years.
(c)   The [operator] must maintain a record of all training provided under 5.91 for each individual. Such records must be retained for as long as the individual is employed by the [operator].
(d) The [operator] must retain records of all communications provided under 5.93 for a minimum of 24 consecutive calendar-months.

IBAC guidance:

IS-BAO 3.5.2 requires operators to develop and maintain SMS operational records as part of its SMS documentation; however no minimum retention periods are specified in the IS-BAO Standard and are left to the operator's discretion taking account of applicable local regulatory requirements. If not already addressed in company manuals, operators need to ensure that all pertinent SMS records are retained in compliance with the requirements of SMSVP 5.97(a) through 5.97(d).

Appendix 1 - SMSVP Internal Assessment Checklist

Operator:	*(name)*	Date:	
SMSVP ref.	**SMSVP Standard**	**Operator ref.**	**Complies?**
5.23(a)	Accountability for safety for the AE, all members of management and employees as per 5.23(a) is contained or referenced in the operator's safety policy.		Yes / No
5.23(a)	The operator's documentation defines accountability for safety for: (2) All members of management in regard to developing, implementing, and maintaining SMS processes within their area of responsibility, including, but not limited to: (i) Hazard identification and safety risk assessment. (ii) Assuring the effectiveness of safety risk controls. (iii) Promoting safety as required in subpart E of the SMSVP Standard. (iv) Advising the accountable executive on the performance of the SMS and on any need for improvement.		Yes / No
5.25(a)	The operator identified an accountable executive who, irrespective of other functions, satisfies the following: (2) Controls the financial resources required for the operations to be conducted under the operator's certificate(s). (3) Controls the human resources required for the operations authorized to be conducted under the operator's certificate(s).		Yes / No
5.25(b)	The accountable executive accomplishes the following: (4) Regularly reviews the operator's safety policy to ensure it remains relevant and appropriate to the operator. (5) Regularly reviews the safety performance of the operator's organization and directs actions necessary to address substandard safety performance in accordance with 5.75.		Yes / No
5.25(c)	The accountable executive designates sufficient management personnel who, on behalf of the accountable executive, are responsible for the following: (1) Coordinate implementation, maintenance, and integration of the SMS throughout the operator's organization. (2) Facilitate hazard identification and safety risk analysis. (3) Monitor the effectiveness of safety risk controls. (4) Ensure safety promotion throughout the operator's organization as required in subpart E of this Standard. (5) Regularly report to the accountable executive on the performance of the SMS and on any need for improvement.		Yes / No
5.27	The manual that contains the ERP is formally approved by the AE, and the operator's Safety Policy refers to the AE's approval of the ERP.		Yes / No

SMSVP ref.	SMSVP Standard	Operator ref.	Complies?
5.27	The operator's emergency response plan addresses the following: (a) Delegation of emergency authority throughout the operator's organization; (b) Assignment of employee responsibilities during the emergency		Yes / No
5.53(a)	(a) When applying safety risk management, the [operator] analyzes the systems identified in 5.51. Those system analyses are used to identify hazards under paragraph (c) of this section, and in developing and implementing risk controls related to the system under 5.55(c).		Yes / No
5.53(b)	In conducting the system analysis, the following information is considered: (1) Function and purpose of the system. (2) The system's operating environment. (3) An outline of the system's processes and procedures. (4) The personnel, equipment, and facilities necessary for the operation of the system.		Yes / No
5.55(d)	The operator evaluates whether the risk will be acceptable with the proposed safety risk control applied before the safety risk control is implemented.		Yes / No
5.71(a)(7)	The operator's hazard identification process includes a confidential employee reporting system in which employees can report hazards, issues, concerns, occurrences, incidents, as well as propose solutions and safety improvements.		Yes / No
5.97(a)	The operator maintains records of outputs of safety risk management processes as described in subpart C of the SMSVP Standard, and retains such records for as long as the control remains relevant to the operation.		Yes / No
5.97(b)	The operator maintains records of outputs of safety assurance processes as described in subpart D of the SMSVP Standard and retains such records for a minimum of 5 years.		Yes / No
5.97(c)	The operator maintains a record of all training provided under 5.91 for each individual and retains such records for as long as the individual is employed by the operator.		Yes / No
5.97(d)	The operator retains records of all communications provided under 5.93 for a minimum of 24 consecutive calendar months.		Yes / No
Assessor:	*(name)*	**Date:**	
Signature:			

Appendix 2 – Tenets of system-thinking

Tenets	Description	Practical implications (i.e., where focus is needed to assess and manage risks)
Multiple actors and levels	Risk is an emergent property of complex socio-technical systems. It is impacted by the decisions of all actors in the system and not just front-line workers.	The risk assessment identifies actors, decisions and actions involved with the provision of the task.
Multiple contributing factors	Risks are usually caused by multiple contributing factors across multiple levels of the organization, not just a single catastrophic decision or action.	Multiple hazards and risks are considered within and between all levels of the system, and not solely by those at the sharp end, or solely by one 'catastrophic' or 'obvious' risk/hazard.
Vertical integration	Risks can result from a lack of vertical integration (i.e., mismatches) across levels of a complex socio-technical system, not just from deficiencies at any one level alone.	The risk assessment enables the deliberate provision of communication opportunities between all actors (i.e., human, machine, software), in relation to hazards and risks, at all levels in the system, and not solely between those positioned at the front line.
Feedback	Lack of feedback also leads to loss of vertical integration across multiple levels. Actors are not able to see the impact of their decisions, so risks are not obvious before an accident.	The risk assessment offers an opportunity for actors in the system to verify that actions, decisions, and communications have been received and understood as intended.
External pressure	Risks are not static and tend to migrate over time under the influence of a cost gradient driven by financial pressure and an aggressive competitive environment. Work practices also migrate under an effort gradient driven by psychological pressure to follow the path of least resistance/effort.	The risk assessment purposefully considers and evaluates potential external pressures impacting actors and artifacts across all levels of the system. The risk assessment process enables new and emerging hazards and risks to be frequently considered and is not simply a repeat of past iterations; irrespective of past accident performance.
Migration of work practices at multiple levels	Risks occur at multiple levels of the organization, not just one level alone.	The risk assessment is adaptive enough to enable ongoing, dynamic risk assessment to occur.
Erosion of defenses through migration of work practices	The migration of work practices over time leads to the gradual erosion of the system's defenses. Risks occur as a combination of this systematic migration and a triggering event, rather than by the occurrence of an unusual action or one-off threats to safety.	The risk assessment is relevant in the context of current work practices, influences, and threats.

THIS PAGE
INTENTIONALLY
LEFT BLANK