Section 1 — Organization and Management System (ORG)

Applicability

Section 1 addresses the organization and management system of an operator for the purpose of ensuring the safety and security of aircraft operations.

Individual ORG provisions or sub-specifications within an ORG provision that:

- Do not begin with a conditional phrase are applicable to all operators unless determined otherwise by the Auditor.
- Begin with a conditional phrase ("If the Operator...") are applicable if the operator meets the condition(s) stated in the phrase.

Many ORG provisions are repeated in one or more other sections of the ISM (as indicated by the ► symbol). Refer to the IOSA Audit Handbook for information relevant to the proper internal auditing of repeated ORG ISARPs.

ORG 2.1.4 in this section is applicable only to an operator that is currently on the IOSA Registry and is being audited for the purpose of registration renewal.

General Guidance

Definitions of technical terms used in this ISM Section 1, as well as the meaning of abbreviations and acronyms are found in the IATA Reference Manual for Audit Programs (IRM).

1 Management and Control

1.1 Management System Overview

ORG 1.1.1

The Operator shall have a management system that has continuity throughout the organization and ensures control of operations and management of safety and security outcomes. (**GM**) ►

Auditor Actions

- ☐ **Identified/Assessed** organizational management system structure.
- ☐ **Assessed** status of conformity with all other ORG management system ISARPs.
- ☐ **Coordinated** to verify status of conformity with management system ISARPs in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Operations, Operator, Organogram, Safety (Operational), Security (Aviation) and State.

A management system is documented in controlled company media at both the corporate and operational levels. Manuals or controlled electronic media are acceptable means of documenting the management system.

Documentation provides a comprehensive description of the scope, structure and functionality of the management system and depicts lines of accountability throughout the organization, as well as authorities, duties, responsibilities and the interrelation of functions and activities within the system for ensuring safe and secure operations.

Acceptable means of documentation include, but are not limited to, organograms (organization charts), job descriptions and other descriptive written material that define and clearly delineate the management system.

Documentation also reflects a functional continuity within the management system that ensures the entire organization works as a system and not as a group of independent or fragmented units (i.e., silo effect).

An effective management system is fully implemented and functional with a clear consistency and unity of purpose between corporate management and management in the operational areas.

The management system ensures compliance with all applicable standards and regulatory requirements. In addition to internal standards and regulations of the State, an operator may also be required to comply with authorities that have jurisdiction over operations that are conducted over the high seas or within a foreign country.

ORG 1.1.2

The Operator shall identify one senior management official as the accountable executive (AE) who is accountable for performance of the management system as specified in ORG 1.1.1 and:

(i) Irrespective of other functions, is accountable on behalf of the Operator for the implementation and maintenance of the safety management system (SMS) throughout the organization;

(ii) Has the authority to ensure the planning and allocation of resources necessary to manage safety and security risks to aircraft operations;

(iii) Has overall accountability for ensuring operations are conducted in accordance with conditions and restrictions of the Air Operator Certificate (AOC), and in compliance with applicable regulations and standards of the Operator. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified** senior management official designated as the AE for the conduct of operations.
- ☐ **Examined** management system structure and organizational lines of accountability.
- ☐ **Examined** job description of designated AE (focus: accountability/responsibilities are as specified in the standard).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Accountability, Accountable Executive (AE), Air Operator Certificate (AOC), Authority, Aircraft Operations, Responsibility, Operations Manual (OM), Safety Management System (SMS), Safety Risk Management and Senior Management.

The requirement for an AE is an element of the Safety Policy and Objectives component of the SMS framework.

The designation of an AE means the accountability for operational quality, safety and security performance is placed at a level in the organization having the authority to take action to ensure the management system is effective. Therefore, the AE is typically the chief executive officer (CEO), although, depending on the type and structure of the organization, it could be a different senior official (e.g. chairperson/member of the board of directors, company owner).

The AE has the authority, which includes financial control, to make policy decisions, provide adequate human and physical resources, resolve operational quality, safety and security issues and, in general, ensure necessary system components are in place and functioning properly.

In terms of resources, the AE would have the overall responsibility for ensuring, not only adequate numbers of personnel, but also that positions within the SMS are filled by personnel in accordance with ORG 1.5.3. Additionally, the AE would be responsible for ensuring the SMS is provided with adequate facilities, workspace equipment and supporting services as specified in ORG 1.5.2.

In an SMS, the AE would typically have:

- Ultimate responsibility and accountability for the safety of the entire operation together with the implementation and maintenance of the SMS;
- Responsibility for ensuring the SMS is properly implemented in all areas of the organization and performing in accordance with specified requirements.

The AE also is responsible for ensuring the organization is in compliance with requirements of applicable authorities (i.e. regulations), as well as its own policies and procedures, which may exceed existing regulations or address areas that are not regulated (e.g. ground handling operations). An operator's policies and procedures are typically published in its Operations Manual (OM).

To ensure that the operator continues to meet applicable requirements, the AE might designate a manager with the responsibility for ensuring activities of the operator are monitored for compliance with the applicable regulatory requirements, as well as any additional requirements as established by the operator, and that these activities are being carried out properly under the supervision of the head of relevant functional areas.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.1.3

If required by the State of the Operator (hereinafter, the State), the Operator shall have post holders within the management system that are acceptable to the Authority and have the responsibility for ensuring, in their respective defined operational areas:

(i) The management of safety and security risks to aircraft operations;

(ii) Operations are conducted in accordance with conditions and restrictions of the AOC, and in compliance with applicable regulations and standards of the Operator. **(GM)** ►

Auditor Actions

- ☐ **Identified** post holders accountable for the conduct of operations.
- ☐ **Examined** management system structure and organizational lines of accountability.
- ☐ **Examined** job descriptions of all post holders throughout the organization (focus: accountability/responsibilities are as specified in the standard).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Post Holder.

Managers in such positions might be referred to as post holders, directors or another title as specified by each State.

ORG 1.1.4

The Operator shall designate a manager who is responsible for the implementation, maintenance and day-to-day administration of the SMS throughout the organization on behalf of the AE and senior management. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified** designated manager for day-to-day administration and oversight of the SMS.
- ☐ **Examined** SMS organizational structure.
- ☐ **Examined** job description of SMS manager (focus: assigned responsibility for organizational implementation of SMS).
- ☐ **Interviewed** SMS manager and/or designated representative.
- ☐ **Other Actions** (Specify)

Guidance

The requirement for a manager that focuses on the administration and oversight of the SMS on behalf of the AE is an element of the Safety Policy and Objectives component of the SMS framework.

The individual assigned responsibility for organizational implementation of an SMS is ideally a management official that reports to the AE. Also, depending on the size, structure and scope of an operator's organization, as well as the complexity of its operations, such individual may be assigned functions in addition to those associated with the SMS manager position provided those functions do not result in a conflict of interest.

The title assigned to the designated manager will vary for each organization. Regardless of title, the manager is the designated organizational focal point for the day-to-day development, administration and maintenance of the SMS (i.e. functions as the SMS *champion*). It is important that such manager has the necessary degree of authority when coordinating and addressing safety matters throughout the organization.

Whereas the designated manager has responsibility for day-to-day oversight of the SMS, overall accountability for organizational safety rests with the AE. Likewise, post holders (refer to ORG 1.1.3) or operational managers always retain the responsibility (and thus are accountable) for ensuring safety in their respective areas of operations.

Note: *Depending on the size of an operator's organization and the complexity of its operations, the responsibilities for implementation and maintenance of the SMS (i.e. fulfillment of the SMS manager role) may be assigned to one or more persons.*

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.1.5–1.1.9 (Intentionally open)

ORG 1.1.10

The Operator shall have an SMS that is implemented and integrated throughout the organization to ensure management of the safety risks associated with aircraft operations. **[SMS] (GM)**

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all standards (not recommended practices) that are identified by the **[SMS]** symbol.*

Auditor Actions

- ☐ **Identified/Assessed** safety management system (SMS) structure.
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Assessed** status of conformity with all ORG SMS standards.
- ☐ **Coordinated** to verify status of conformity with SMS standards in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of IOSA Operator, and State Safety Program (SSP).

IOSA specifications for an operator's SMS are derived from the SMS Framework, which is published in Annex 19 to the Convention on International Civil Aviation (ICAO Annex 19). The SMS Framework specifies the four major components and 12 elements that make up the basic structure of an SMS.

Where applicable, an SMS is designed and implemented in accordance with the State Safety Program (SSP). The manner in which the elements of SMS are implemented typically reflects the size and complexity of the operator's organization.

In general, an SMS is designed and implemented to:

- Identify safety hazards in operations;
- Ensure remedial action is implemented to control safety risks;
- Provide for ongoing monitoring and assessment of safety performance;
- Make continual improvement to the level of safety in operations.

The specific requirements for each operator's SMS will normally be found in the regulations associated with the SSP. In addition, states typically publish guidance designed to assist operators in the implementation of SMS.

A description of an operator's SMS is contained in documentation as specified in ORG 2.5.4.

Expanded guidance may be found in the ICAO Safety Management Manual (ICAO SMM), Document 9859.

1.2 Management Commitment

ORG 1.2.1

The Operator shall have a corporate safety policy that reflects the organizational commitment to safety, including the promotion of a positive safety culture. Such policy shall be communicated throughout the organization and include the following:

(i) A statement about the provision of the necessary resources for the implementation of the safety policy;

(ii) A commitment to the continual improvement of the organization and the management system;

(iii) A commitment to a periodic review of the policy to ensure its continued relevance to the organization. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** corporate safety policy (focus: organizational commitment to safety/provision of necessary resources).
- ☐ **Interviewed** AE, SMS manager and/or designated management representative.
- ☐ **Examined** examples of corporate communication: (focus: safety policy communicated throughout organization).
- ☐ **Coordinated** to verify communication of safety policy in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Quality Management System (QMS).

The requirement for an operator to have a defined safety policy is an element of the Safety Policy and Objectives component of the SMS framework.

The policy of an operator reflects the commitment of senior management to ensuring continual measurement and evaluation as well as the implementation of changes that improve the management system and the culture. Ideas for improvement may come from internal and external sources. Therefore, the organization would be constantly monitoring all sources and willing to make changes as necessary to keep the management system refreshed and strongly focused on improving operational quality, safety and security performance.

The safety policy typically also reflects the commitment of senior management to ensure:

- Compliance with applicable regulations and standards of the Operator;
- The management of safety and security risks to aircraft operations;
- The promotion of safety and security awareness;
- Continual improvement of operational performance;
- Regular review of safety performance indicators by senior management;
- Regular analysis of malfunctions or undesirable operational results;
- Follow-up of corrective actions and their effectiveness in improving operational performance.

An SMS, as well as a Quality Management System (QMS) and Security Management System (SeMS), are integrated components of an operator's overall management system and would typically be subjected to protocols for continual improvement in accordance with the operator's policy.

The corporate safety policy may be documented in the OM or other controlled document. To enhance effectiveness, the policy is communicated and made visible throughout the organization through the dissemination of communiqués, posters, banners and other types of media in a form and language that can be easily understood. To ensure continuing relevance, the corporate policy is typically reviewed for possible update a minimum of every two years.

Consistent with the structure and complexity of the operator's organization, the corporate safety policy may be issued as a stand-alone policy or combined with the safety reporting policy specified in ORG 1.2.2.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.2.2

The Operator shall have a corporate safety reporting policy that encourages personnel to report hazards to aircraft operations and, in addition, defines the Operator's policy regarding disciplinary action, to include:

(i) Types of operational behaviors that are unacceptable;

(ii) Conditions under which disciplinary action would not apply. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** corporate safety reporting policy (focus: personnel urged to report operational hazards; definition of disciplinary policy/potential disciplinary actions).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Coordinated** to verify implementation of safety reporting in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Just Culture.

The requirement for an operator to have a safety reporting policy is an element of the Safety Policy and Objectives component of the SMS framework.

Safety reporting is a key aspect of SMS hazard identification in the management of risk.

Such a policy is typically documented in operations manuals or other controlled documents.

Consistent with the structure and complexity of the operator's organization, the safety reporting policy may be issued as a stand-alone policy or combined with the safety policy that is specified in ORG 1.2.1.

A safety reporting policy encourages and perhaps even provides incentive for individuals to report hazards and operational deficiencies to management. It also assures personnel that their candid input is highly desired and vital to safe and secure operations.

It is important that the operator provides appropriate protections to encourage personnel to report what they see or experience. For example, enforcement action may be waived for reports of errors or, under certain circumstances, even rule breaking. It should be clearly stated that reported information will be used solely to support the enhancement of safety. The intent is to promote an effective reporting culture and proactive identification of potential safety deficiencies.

An effective reporting culture exists when personnel have confidence that their reports are used to improve operational safety by learning from mistakes and system flaws, and thus improve the safety of operations. To that end, an operator's safety reporting policy would typically incorporate the principles of Just Culture.

The safety reporting policy is typically reviewed periodically to ensure continuing relevance to the organization.

Refer to ORG 3.1.2 and 3.1.3, both of which address operational safety reporting.

ORG 1.2.3

The Operator shall have a policy that informs operational personnel throughout the organization of their responsibility to comply with the applicable laws, regulations and procedures in all locations where operations are conducted.

Auditor Actions

- ☐ **Identified/Assessed** corporate compliance policy (focus: requirement for organizational compliance with applicable laws/regulations/procedures by operational personnel).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Coordinated** to verify implementation of compliance policy in all operational areas.
- ☐ **Other Actions** (Specify)

1.3 Roles and Responsibilities

ORG 1.3.1

The Operator shall ensure the management system defines the safety accountability, authorities and responsibilities of management and non-management personnel throughout the organization, and specifies:

(i) The levels of management with the authority to make decisions regarding risk tolerability with respect to the safety and/or security of aircraft operations;

(ii) Responsibilities for ensuring operations are conducted in accordance with applicable regulations and standards of the Operator;

(iii) Lines of safety accountability throughout the organization, including direct accountability for safety and/or security on the part of senior management. **[SMS] (GM) ►**

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

☐ **Identified/Assessed** defined safety accountability/authorities/responsibilities for management/non-management personnel (focus: definitions apply to personnel throughout the organization).

☐ **Interviewed** AE and/or designated management representative(s).

☐ **Coordinated** to verify defined accountability/authorities/responsibilities in all operational areas.

☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of IOSA Audit Handbook (IAH) and Risk Tolerability.

The definition of authorities and responsibilities of management and non-management personnel is an element of the Safety Policy and Objectives component of the SMS framework.

In the context of the management system, the following typically apply:

- Accountability is the obligation to accept ultimate responsibility and be answerable for decisions and policies, and for the performance of applicable functions, duties, tasks or actions. Accountability may not be delegated.
- Authority is the delegated power or right to command or direct activities, and to make decisions.
- Responsibility is the obligation to execute or perform assigned functions, duties, tasks and/or actions. Responsibility may be accompanied by an appropriate level of delegated authority.

In the context of an SMS, the assignment of responsibility to individual personnel means such personnel are ultimately accountable for safety performance, whether at the overall SMS level (accountable executive) or at specific product and/or process levels (other applicable members of management).

An effective management system ensures that responsibilities, and thus accountability, for safety and security are allocated to relevant management and non-management personnel that perform safety- or security-related functions, or that have a defined role in either the SMS or the SeMS. Responsibilities and accountability are typically defined in the functional job description for such personnel and are designed to flow from corporate senior management into all operational areas of the organization.

Responsibilities and accountability are normally described and communicated in a manner that ensures a clear understanding throughout the organization. Organization charts, or organograms, are typically used to depict the functional reporting system of an organization, and thus are an acceptable means for defining the flow (or “lines” as depicted on an organogram) of responsibilities and accountability within the management system.

Management positions critical to operational safety or security may require enhanced job descriptions or terms of reference that reflect specialized requirements inherent in certain key

positions. Such specialized requirements would include any delegation of authority exercised by personnel on behalf of an authority (e.g. designated or authorized flight examiner).

Compliance with regulatory requirements, as well as internal policies and procedures, is an essential element of a safe and secure operational environment. The responsibility for ensuring compliance with both regulatory and internal requirements is specified and assigned within the management system. Job descriptions, terms of reference and operating manuals are examples of appropriate locations for documenting management system responsibilities.

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.3.2

The Operator shall have a process or procedure for the delegation of duties within the management system that ensures managerial continuity is maintained when operational managers including, if applicable, post holders are unable to carry out work duties. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** processes for management system delegation of duties (focus: processes maintain managerial continuity during periods when corporate/operational managers are unable to perform work duties).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Coordinated** to verify processes for management system delegation of duties in all operational areas.
- ☐ **Examined** example(s) of delegation of duties when managers have been unable to perform work duties.
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for an operator to have a process or procedure that ensures a specific person (or perhaps more than one person) is identified to assume the duties of any operational manager that is or is expected to be, unable to accomplish assigned work duties. An operator may have nominated deputies in place or a process for ensuring the appointment of a temporary replacement.

For the purpose of this provision, the use of telecommuting technology and/or being on call and continually contactable are acceptable means for operational managers to remain available and capable of carrying out assigned work duties.

A notification of such delegation of duties may be communicated throughout the management system using email or other suitable communication medium.

ORG 1.3.3

The Operator shall ensure a delegation of authority and assignment of responsibility within the management system for liaison with regulatory authorities, original equipment manufacturers and other operationally relevant external entities. **(GM)** ►

Auditor Actions

- ☐ **Identified** corporate management individuals with authority for liaison with regulators/other external entities.
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Interviewed** selected manager(s) with authority for liaison with regulators/other external entities.
- ☐ **Coordinated** to identify managers with authority for liaison with external entities in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

To ensure the communication and coordination with external entities is consistent and appropriate, liaison with operationally relevant external entities is normally controlled through the delegation of authority and assignment of responsibility to specifically named management personnel. Such authorities and responsibilities would normally be included in the job descriptions of the applicable managers.

1.4 Safety Performance

ORG 1.4.1

The Operator shall have a process to define safety objectives. Such safety objectives shall:

(i) Reflect the Operator's commitment to maintain or continuously improve the overall effectiveness of the SMS;

(ii) Be communicated throughout the organization;

(iii) Be periodically reviewed to ensure they remain relevant and appropriate to the Operator. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** organizational program for setting safety objectives.
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected safety objectives currently valid.
- ☐ **Examined** selected records/documents that identify tracking of safety objectives.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Safety Assurance and Safety Objective.

Defining safety objectives is an element of the Safety Policy and Objectives component of the SMS framework.

Safety objectives provide direction to the operator's safety management activities and would therefore be consistent with the safety policy that sets out the organization's high-level safety commitment.

A safety objective is a high-level statement that typically expresses a desired safety outcome that is to be achieved over a defined period of time (e.g. one year).

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.4.2

The Operator shall have processes for setting safety performance indicators (SPIs) and, as applicable, safety performance targets (SPTs) as means to monitor its safety performance, the achievement of its safety objectives and to validate the effectiveness of safety risk controls. **[SMS] (GM)** ►

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** organizational program for setting SPIs and SPTs (focus: program defines/requires development/application of SPIs; measures used to track/monitor operational safety performance/validate safety risk controls).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected SPIs and SPTs (focus: SPIs/SPTs are aligned with safety objectives and are being used to monitor operational performance).
- ☐ **Examined** selected records/documents that identify tracking of SPIs and SPTs (focus: tracking used to assess/monitor operational safety performance, assess/validate risk control effectiveness).

- ☐ **Coordinated** to verify implementation of SPIs and SPTs in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Safety Performance Indicator (SPI) and Safety Performance Target (SPT).

Setting SPIs in support of the operator's safety objectives is an element of the Safety Assurance component of the SMS framework.

SPIs and SPTs are used by an operator to track and compare its operational performance against the achievement of its safety objectives and to focus attention on the performance of the organization in managing operational risks and maintaining compliance with relevant regulatory requirements.

SPTs define short-term and medium-term safety performance management desired achievements. They act as 'milestones' that provide confidence that the organization is on track to achieving its safety objectives and provide a measurable way of verifying the effectiveness of safety performance management activities. The setting of SPTs is normally accomplished after considering what is realistically achievable and, where historical trend data are available, the recent performance of the particular SPI.

It is not always necessary or appropriate to set or define SPTs as there could be some SPIs that are better monitored for trends rather than against a targeted number. Safety reporting is an example of when having a target could either discourage people not to report (if the target is not to exceed a number) or to report trivial matters to meet a target (if the target is to reach a certain number).

In addressing operational performance, meaningful indicators might focus on lower level (i.e. lower consequence) occurrences or conditions that are considered by the operator to be precursors to more serious events. SPIs may be specific to a certain area of operations or may be broad and apply to the entire system.

In addressing compliance, meaningful indicators, as a minimum, would focus on compliance with significant regulatory requirements (as determined by the operator) in all operational areas.

SPIs may be set in almost any operations or maintenance area and are usually expressed as a reduction in the rate or number of specifically identified occurrences or conditions.

Some possible examples of operational occurrences or conditions, listed by operational discipline, that could be monitored using SPIs include:

- Flight operations (e.g. takeoff and landing tail strikes, unsatisfactory line or training evaluations, unstabilized approaches, runway incursions/excursions);
- Operational control (e.g. flight diversions due to fuel);
- Engineering and maintenance (in-flight engine shutdowns, aircraft component/equipment failures, diversions due to maintenance errors, damage caused by maintenance);
- Cabin operations (inadvertent slide deployments);
- Ground handling (aircraft damages due to vehicles or equipment);
- Cargo operations (dangerous goods spills);
- Operational security (unauthorized interference or access events).

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

1.5 Resource Management

ORG 1.5.1

The Operator shall ensure the management system includes planning processes for operations which:

(i) Define desired operational safety and security objectives;

(ii) Address operational resource allocation requirements;

(iii) Take into account requirements originating from applicable external sources, including regulatory authorities and original equipment manufacturers. **(GM)**

Note: *The definition of desired safety objectives as specified in item (i) shall take into account and be consistent with the Operator's safety policy.*

Auditor Actions

- ☐ **Identified/Assessed** planning processes for operations (focus: planning includes defining operational safety/security goals/objectives, allocates necessary resources).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Examined** selected planning records/documents (focus: planning addresses internal/external operational safety/security objectives/requirements).
- ☐ **Coordinated** to verify planning processes take into account all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Management system planning processes are necessary to ensure sufficient resources are in place to meet internal operational safety and security requirements, as well as to meet requirements from external sources, such as regulatory authorities and equipment manufacturers. Resource requirements would typically be determined through risk assessment, management review or other management processes.

Planning processes typically result in the generation of goals, objectives or other types of performance measures that would represent the operational safety and security outcomes an operator plans for and desires to achieve.

Defined safety objectives reflect the service provider's commitment to maintain or continuously improve the overall effectiveness of its SMS, and typically form the basis for the setting of SPIs (see ORG 1.4.1 and 1.4.2).

Planning processes may be part of, or associated with, the budgetary process, which typically take place prior to the start of a calendar or fiscal year and involve decisions that result in a plan for capital and operating expenditures to support operations.

Expanded guidance regarding the setting of safety objectives may be found in the ICAO SMM, Document 9859.

ORG 1.5.2

The Operator shall ensure existence of the facilities, workspace, equipment and supporting services, as well as work environment, necessary to satisfy operational safety and security requirements. **(GM)** ►

Note: *Conformity with this ORG provision and repeats in other ISM sections does not require specifications to be documented by the Operator.*

Auditor Actions

- ☐ **Observed/Assessed** physical resources/services (focus: adequacy to meet operational needs).
- ☐ **Interviewed** AE or designated management representative(s).
- ☐ **Coordinated** to verify adequacy of physical resources/services in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

The management system would identify, typically through policy, risk assessment, management review or other means, the infrastructure and resource requirements that would be necessary to deliver safe and secure operations, to include operations and maintenance support facilities, services and equipment appropriate for the area, such as:

- Buildings, workspaces and associated utilities;
- Facilities for people in the organization;
- Support equipment, including tools, hardware and software;
- Support services, including transportation and communication.

A suitable work environment satisfies human and physical factors and considers:

- Safety rules and guidance, including the use of protective equipment;
- Workplace location(s);
- Workplace temperature, humidity, light, air flow;
- Cleanliness, noise or pollution.

Implementation of this provision (i.e. adequacy of physical resources, work environment) is typically assessed through observations made by auditors during the course of the on-site audit.

△ **ORG 1.5.3**

The Operator shall have a selection process for management and non-management positions within the organization that require the performance of functions relevant to the safety or security of aircraft operations. Such process shall ensure candidates are selected on the basis of knowledge, skills, training and experience appropriate for the position. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** standards/processes for hiring/selection of management/non-management personnel (focus: safety/security positions relevant to aircraft operations are filled by personnel with qualifications appropriate for position).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Interviewed** selected personnel that perform safety/security functions relevant to aircraft operations.
- ☐ **Coordinated** to verify implementation of personnel selection standards/processes in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Prerequisite criteria for each position, which would typically be developed by the operator, and against which candidates would be evaluated, ensure personnel are appropriately qualified for management system positions and operational roles in areas of the organization critical to safe and secure operations.

ORG 1.5.4

The Operator shall ensure personnel who perform functions relevant to the safety or security of aircraft operations are required to maintain competence on the basis of continued education and training and, if applicable for a specified position, continue to satisfy any mandatory technical competency requirements. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** standards/processes for maintaining competency of personnel in functions relevant to safety/security of aircraft operations (focus: standards specify continuing education/training, meeting technical requirements).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Coordinated** to verify application of competency standards.
- ☐ **Other Actions** (Specify)

Guidance

Positions or functions within an airline organization considered 'operationally critical' are those that have the potential to affect operational safety or security. This definition includes management positions and any positions or functions that may affect the airworthiness of aircraft.

Typically, training programs are implemented to ensure personnel throughout the organization are qualified and competent to perform individual duties.

Some management positions within airline operations may require an individual to maintain a technical competency as a requirement for being assigned to the position. For example, it may be specified that certain management positions within Flight Operations may only be filled by individuals who are qualified flight crew members. Similar situations could exist within Cabin Operations, Engineering and Maintenance or other operational disciplines.

In such cases, the job description specifies the requirement for maintaining technical competency, and adequate opportunity is provided to fulfill the requirement.

△ **ORG 1.5.5**

The Operator shall have a policy that addresses the use of psychoactive substances by personnel that perform operational functions and, as a minimum:

(i) Prohibits the exercise of duties while under the influence of psychoactive substances;

(ii) Prohibits the problematic use of psychoactive substances;

(iii) Requires that all personnel who are identified as engaging in problematic use of psychoactive substances are removed from operational functions;

(iv) Conforms to the requirements of the Authority, if applicable. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** policy that addresses use of psychoactive substances by operational personnel.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Interviewed** operational personnel (focus: familiarity with psychoactive substance policy).
- ☐ **Other Actions** (Specify)

Guidance

△ Refer to the IRM for the definitions of Biochemical Testing, Psychoactive Substance and Problematic Use of Substances.

△ Personnel that perform operational safety and security functions as specified in this provision refers to persons in all operational disciplines who perform a function that, if performed improperly, could endanger the safety of aircraft operations. This includes operational personnel in all areas (flight crew, cabin crew, flight dispatch personnel (FOO/FOA), maintenance, ground handling, cargo, security).

△ Operators subject to laws or regulations of the State that preclude the publication of a psychoactive substance prohibition policy as specified in this provision may demonstrate an equivalent method of ensuring that personnel engaging in problematic use of psychoactive substance abuse do not exercise their duties and are removed from safety-critical functions.

Re-instatement to safety-critical duties could be possible after cessation of the problematic use and upon determination that continued performance of such duties is unlikely to jeopardize safety.

Some of the specifications of this provision related to flight and cabin crews may be addressed through implementation of a scheduling policy in accordance with FLT 3.4.2 and CAB 3.1.7.

Examples of other subjects that might be addressed in a comprehensive and proactive policy include:

- Education regarding the use of psychoactive substances;
- Identification, treatment and rehabilitation;
- Employment consequences of problematic use of psychoactive substances;

- Biochemical testing;
- Requirements of ICAO and the Authority.

Additional guidance may be found in the ICAO Manual on Prevention of Problematic use of Substances in the Aviation Workplace (Doc 9654-AN/945).

ORG 1.5.6

The Operator *should* have a policy that requires personnel who perform operational functions critical to the safety of aircraft operations to be physically and medically fit for duty. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** policy that requires personnel in operational functions critical to the safety of aircraft operations to be physically/medically fit for duty (focus: methods used to determine physical/medical fitness).
- ☐ **Interviewed** AE or designated management representative(s).
- ☐ **Coordinated** to verify policy is implemented in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Operational Function (Aircraft Operations).

☐ **ORG 1.5.7**

The Operator *should* have a procedure to ensure screening or testing for psychoactive substances is performed on prospective operational personnel, unless such screening or testing is performed or prohibited by the State. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** procedure used for screening/testing operational personnel for psychoactive substances.
- ☐ **Interviewed** the responsible manager(s) in operational areas.
- ☐ **Examined** selected records of screening/testing for psychoactive substances.
- ☐ **Other Actions** (Specify)

1.6 Outsourcing Management

ORG 1.6.1

If the Operator has external service providers conduct outsourced operational functions, the Operator *should* ensure a service provider selection process is in place that ensures:

(i) Relevant safety and security selection criteria are established;

(ii) Service providers are evaluated against such criteria prior to selection. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** selection process for external service providers.
- ☐ **Interviewed** manager and/or designated management representative(s).
- ☐ **Examined** selected records/documents that demonstrate application of the selection process.
- ☐ **Coordinated** to verify implementation of selection process in all operational areas.
- ☐ **Other Actions** (specify)

Guidance

The intent of this provision is for an operator to define relevant safety and security criteria for use in the evaluation and potential selection of service providers. This is the first step in the management of external service providers and would take place prior to the operator signing an agreement with a provider. The process need be applied only one time leading up to the selection of an individual service provider. The specified evaluation would typically be done as part of a tendering process

once one or more potential service providers have been identified for consideration and are being vetted.

The provision specifies relevant safety and security selection criteria, but an operator would always have the discretion to include additional selection criteria that might not be directly related to the safety or security of the services to be provided.

The selection process would normally be applied when there is a need for a new service provider, such as when opening a new destination or outsourcing a service that has previously been performed using internal resources. It might also be applied when the term of an existing service provider contract is about to expire and one or more replacement providers are being considered for a new agreement.

The focus of the selection process is on the contracted services with a provider over an extended time period as specified in an agreement. It is possible that there could be the need for an ad-hoc selection process should an existing provider be unable to deliver contracted services due to unplanned or unexpected circumstances (e.g. unable to deliver the contracted services due to loss of accreditation, financial problems, labor disruption). In such case, an alternative process might be required because there is a lack of time to carry out the full process as specified.

Also, the specified selection process might have limited value at a location where there is only one service provider available (e.g. station monopoly, government/authority-provided services). In such situations, the operator would need to apply sound risk management to determine whether its safety and security requirements will be satisfied by the only available service provider should it choose to continue conducting operations at the location.

ORG 1.6.2

The Operator shall have processes to ensure a contract or agreement is executed with external service providers that conduct outsourced operational functions for the Operator. Such contract or agreement shall identify specific documented requirements that can be monitored by the Operator to ensure the safety and/or security of operations are being fulfilled by the service provider. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** processes for contract/agreement production/execution with external service providers that conduct outsourced operations, maintenance security functions.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected outsourcing contracts/agreements (focus: inclusion of or reference to specific requirements applicable to service providers).
- ☐ **Coordinated** to verify implementation of service provider contract/agreement processes in applicable operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Outsourcing and Service Level Agreement (SLA).

An operator would always retain full responsibility for ensuring an outsourced operational function is performed properly by an external provider, even if such provider is the parent organization or an affiliate of the operator.

A contract or agreement is necessary to ensure details of the operational functions to be performed by the external service provider are formally documented. The contract or agreement not only sets forth commercial terms, but also specific safety and/or security requirements pertaining to the services the provider is expected to perform. These requirements typically form the basis for the monitoring of the service provider by the operator.

Examples of specific documented requirements could include the following:

- Processes or procedures from the operator's own documentation system (e.g. operational manuals, working instructions) that can be included in the contract by reference.
- Infrastructure, resource or certification requirements (e.g. number of personnel, certification standards for equipment, support equipment standards).

- SPIs that specify a maximum number of occurrences or deviations), which could be based on the operator's own SPIs in accordance with ORG 1.4.2.

The structure of contracts or agreements will vary with individual operators and, depending on such structure, defined specific requirements may or may not be contained in any of the contractual documents. When the specific requirements are not contained in the contract, they may be defined (in technical terms) in a controlled document that is part of the operator's documentation system, and then conveyed to the provider (perhaps periodically) in a manner that ensures understanding. Such controlled documents are typically identified in the contract by reference.

Note: *For the purpose of this provision, the contract or agreement as specified above may comprise multiple parts, including the basic document that sets forth legal and commercial terms and, as applicable, other associated documents that state terms or conditions of service (e.g. appendices, addenda, service level agreement).*

1.7 Emergency Response

ORG 1.7.1

The Operator shall have a corporate emergency response plan (ERP) for the central management and coordination of all activities necessary to respond to a major aircraft accident or other type of adverse event that results in fatalities, serious injuries, considerable damage and/or a significant disruption of aircraft operations. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** corporate emergency response plan (ERP) (focus: plan suitable for organizational response to major aircraft accident/other adverse event).
- ☐ **Interviewed** designated ERP manager.
- ☐ **Coordinated** to verify implementation of ERP in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Emergency Response Plan (ERP) and Public Health Emergency.

Emergency response planning is an element of the Safety Policy and Objectives component of the SMS framework.

An emergency (or crisis) response plan is based upon an assessment of risk appropriate to the size and type of operations, and includes consideration of a major aircraft accident and other potential, aircraft and/or non-aircraft events that would require a full corporate emergency response.

In some states, emergency or crisis response is assumed by a governmental authority rather than by the operator. In such case, an emergency response plan focuses on and addresses interaction with and/or participation in the governmental response to an emergency or crisis.

As a best practice, an operator might consider defining in its ERP an appropriately coordinated response to a public health emergency.

An effective ERP includes industry best practices and ensure community expectations are addressed. Additionally, an ERP:

- Specifies general conditions for implementation;
- Provides a framework for an orderly implementation;
- Ensures proper coordination with external entities at all potential locations (refer to ORG 1.7.4);
- Addresses all potential aspects of an event, including casualties;
- Ensures regulatory requirements associated with specific events are satisfied;
- Provides a scenario for the transition back to normal operations;
- Ensures regular practice exercises as a means to achieve continual improvement (refer to ORG 1.7.8 and ORG 1.7.9).

IATA provides a guide for use by operators in addressing a public health emergency. Such document, titled Emergency Response Plan and Action Checklist, may be found at http://www.iata.org/whatwedo/safety/health/Pages/diseases.aspx.

ORG 1.7.2

The Operator shall have a designated manager with appropriate qualifications and authority to manage and be responsible for the development, implementation and maintenance of the corporate ERP. **(GM)**

Auditor Actions

- ☐ **Identified** designated corporate ERP manager.
- ☐ **Examined** job description of ERP manager (focus: background/duties/responsibilities).
- ☐ **Interviewed** corporate ERP manager.
- ☐ **Other Actions** (Specify)

Guidance

The exact title of the manager designated as responsible for the corporate ERP may vary depending on the organization.

In order to manage a corporate ERP, an individual's qualifications would typically include training and background experience that ensures the requisite knowledge in emergency response principles. Such experience and knowledge is necessary, even though various ERP functions are typically delegated to designated personnel throughout the management system.

ORG 1.7.3

If the Operator has individual departmental or station emergency response plans within the organization, the Operator shall ensure such individual plans are coordinated with the overall corporate emergency response plan under the ERP manager. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) for coordinating departmental/station ERPs.
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Examined** ERP for selected stations (focus: station ERP is coordinated with corporate ERP).
- ☐ **Other Actions** (Specify)

Guidance

Certain operational departments might have individual ERPs, especially where departments are located remotely (e.g. maintenance or cargo). Likewise, station ERPs might be individually tailored to meet varying requirements at each station. Therefore, coordination is always required to ensure each individual ERP within an operator's organization contains or addresses the applicable common elements of the corporate ERP.

ORG 1.7.4

The Operator shall ensure the ERP as specified in ORG 1.7.1 includes provisions for the appropriate coordination with the emergency response plans of other applicable organizations relevant to the particular event or crisis. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** ERP transition processes (focus: plan includes transition from normal-emergency/and emergency-normal operations; coordination with relevant external organizations).
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Other Actions** (Specify)

Guidance

Coordination of emergency response planning is an element of the Safety Policy and Objectives component of the SMS framework.

An ERP typically defines:

- Coordination procedures for action by key personnel;
- External entities that will interact with the organization during emergency situations;
- ERPs of external entities that will require coordination;
- Method(s) of establishing coordination with external ERPs.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 1.7.5

The Operator shall have published procedures and assigned responsibilities to ensure a coordinated execution of the corporate ERP. **(GM)**

Auditor Actions

☐ **Identified/Assessed** procedures/responsibilities for execution of corporate ERP.

☐ **Interviewed** designated corporate ERP manager.

☐ **Coordinated** to verify procedures/assigned responsibilities for ERP execution in all operational areas.

☐ **Other Actions** (Specify)

Guidance

Personnel are typically assigned with specific responsibilities throughout the organization for the implementation of procedures associated with the ERP. Such responsibilities and procedures might include:

- Assemblage of required personnel;
- Travel arrangements, as required;
- Provision of facilities, equipment and other resources;
- Humanitarian and other assistance to individuals involved in the event, as required;
- Management of continuing normal operations;
- Control of areas impacted by the event, as applicable;
- Liaison with relevant authorities and other external entities.

The following areas would normally be considered in developing plans for liaison with external entities associated with any event:

- Fire;
- Police;
- Ambulance;
- Coast guard and other rescue agencies;
- Hospitals and other medical facilities;
- Medical specialists;
- Civil aviation or defense agencies;
- Poison control centers;
- Chemical or radiation specialists;
- Environmental agencies;
- Insurance companies.

Additionally, contact and arrangements are typically made with certain operational business partners, including code share and wet lease operators.

ORG 1.7.6

The Operator shall have a process in the ERP to provide an accurate manifest to the appropriate authorities in the event of an aircraft accident. Such manifest shall list crew members, passengers and cargo, to include dangerous goods.

Auditor Actions

- ☐ **Identified/Assessed** ERP process for providing accurate manifest to authorities in the event of aircraft accident.
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Identified** specific person/function with assigned responsibility for providing accurate manifest to authorities in the event of aircraft accident.
- ☐ **Other Actions** (Specify)

ORG 1.7.7

The Operator *should* ensure all personnel with responsibilities under the ERP are appropriately trained and qualified to execute applicable procedures. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** training/qualification program for ERP personnel.
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Examined** training curriculum for ERP personnel (focus: training subjects appropriate for role in ERP).
- ☐ **Examined** selected training/qualification records of ERP personnel (focus: completion of ERP training).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Family Assistance.

Training for personnel with responsibilities under the ERP could be conducted externally or in-house by an operator's own qualified staff, and would typically include drills, desktop exercises, and/or simulations. Attendees typically include both management and operational personnel from the headquarters and, as applicable to the operator's structure, station locations.

Ideally, specific and/or personalized training would also be conducted for key senior managers (e.g. CEO).

Training programs are generally tailored for personnel based on the role performed under the ERP. Typically, persons involved in family assistance and crisis communications, as well as members of the corporate emergency response group or committee (as applicable), would be required to complete ERP training.

The curriculum for ERP training normally includes general subjects associated with emergency response management, as well as role-specific subjects that address issues associated with:

- Family assistance/special assistance;
- Cultural sensitivity;
- Telephone enquiry;
- Team call-out and assembly;
- Crash site discipline;
- Effects retrieval.

ORG 1.7.8

The Operator shall ensure the corporate ERP is rehearsed periodically to:

(i) Familiarize personnel with responsibilities and procedures;

(ii) Ensure ready functionality of all equipment and facilities;

(iii) Expose deficiencies in the plan and its execution, and ensure such deficiencies are addressed. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** plan for corporate ERP rehearsal (focus: definition of rehearsal type/schedule; rehearsals include use of applicable personnel/facilities/equipment).
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Examined** selected records of ERP rehearsals (focus: implementation/completion of ERP rehearsals).
- ☐ **Other Actions** (Specify)

Guidance

The ERP typically has provisions that ensure all aspects of the ERP are rehearsed or practiced at regular intervals, and practice exercises include the involvement of all personnel that would be called upon during an actual emergency or crisis situation. In some locations, the extent of ERP rehearsals might be limited by the relevant authority. In such cases, a modified rehearsal that ensures overall ERP readiness in accordance with the specifications stated in this provision is acceptable.

Rehearsal of an ERP typically results in the discovery of, and thus an opportunity to correct, deficiencies in the plan. Such deficiencies could include outdated contact information (e.g. names, telephone numbers, email addresses) and/or plan execution discrepancies (e.g. organizational changes, personnel turnover).

The results of rehearsals or practice exercises are normally recorded and analyzed, and then used as the basis for continual improvement of the plan (refer to ORG 1.7.9).

ORG 1.7.9

The Operator *should* have a process for a detailed debriefing and critique whenever the ERP is executed, either as a rehearsal or in response to an actual event. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process for debriefing/critique after execution of ERP (focus: debriefing/critique part of actual/rehearsed ERP implementation).
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Examined** selected records of detailed debriefing/critique after rehearsal/actual ERP activation.
- ☐ **Other Actions** (Specify)

Guidance

Such process ensures vital information is communicated to regulatory authorities, corporate management, operational personnel and the local community whenever the ERP is activated, whether for an actual event or for a rehearsal.

If recommendations for corrective action or other changes result from activation of the plan, there is typically a process for providing a de-briefing to relevant internal and external entities to ensure awareness and consideration of such recommendations.

ORG 1.7.10

The Operator *should* have the ready availability of a facility for use as an emergency management center (EMC) with sufficient space, furnishings and equipment to successfully manage the execution of the corporate ERP.

Auditor Actions

- ☐ **Observed/Assessed** emergency management center (focus: adequate space/furnishings/equipment to manage ERP and associated resources).
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Other Actions** (Specify)

ORG 1.7.11

The Operator *should* have procedures under the corporate ERP that ensure a central coordination and control of all communications with external entities. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** ERP procedures for central coordination/control of communications with external entities.
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Other Actions** (Specify)

Guidance

A vital aspect of an effective ERP is ensuring a controlled and consistent message to external entities, especially the news media. The ERP would typically include the designation of an individual or group as the central point of control for all external communication. Additionally, authorization and responsibilities would be assigned to certain personnel within the organization to act as the point(s) of contact for communication with specified external entities.

ORG 1.7.12

The Operator *should* have procedures and resources immediately available under the corporate ERP that provide for, in the event of an emergency:

(i) The establishment of command posts (CPs) at line stations or remote locations;

(ii) A telephone enquiry center capable of handling the potential volume of calls expected with emergency events;

(iii) Dedicated equipment and material necessary for successful execution of the corporate ERP;

(iv) The dispatch, on short notice, of humanitarian teams to appropriate location(s) to attend to individuals in need of assistance;

(v) Assistance to passengers, crew and their families. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** resources available under corporate ERP (focus: local command posts; adequate communication capability; humanitarian personnel/teams; passenger/crew/family assistance).
- ☐ **Interviewed** designated corporate ERP manager.
- ☐ **Observed** examples of resources available in the event of ERP activation.
- ☐ **Other Actions** (Specify)

Guidance

In addition to a centralized EMC as specified in ORG 1.7.10, one or more CPs (normally on standby mode) may be established at or near the crisis site. Other resources would typically include, as a minimum:

- Adequate office furnishings and supplies;
- Necessary communications equipment (e.g. computers, telephones, printers, facsimile);
- Required reference documents (e.g. emergency response checklists and procedures, company manuals, airport emergency plans, telephone lists).

Assistance to families typically requires dedicated policies and procedures, as well as the resources necessary to provide family notification and satisfy the critical aspects of logistical support (e.g. transportation, lodging, meals, security, communications, and incidental expenditures).

Refer to the following documents for detailed guidance that addresses family assistance:

- ICAO Doc 9859, Safety Management Manual (SMM).
- ICAO Circular 285, Guidance on Assistance to Aircraft Accident Victims and Their Families.
- ICAO Doc 9998, Policy on Assistance to Aircraft Accident Victims and their Families.

2 Assurance, Monitoring and Documentation Control

2.1 Quality Assurance

ORG 2.1.1

The Operator shall have a quality assurance program that provides for the auditing of the management system of operations and maintenance functions to ensure the organization is:

(i) Complying with applicable regulations and standards;

(ii) Satisfying stated operational needs;

(iii) Identifying areas requiring improvement;

(iv) Identifying hazards to operations;

(v) Assessing the effectiveness of safety risk controls. **[SMS] (GM)** ►

Note: *If the quality assurance audit function is performed by an external organization, the Operator, as the AOC holder, shall be responsible for ensuring the quality assurance program is in conformity with the specifications of this provision.*

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** quality assurance program (focus: role/purpose within organization/SMS; definition of audit program scope/objectives; description of program elements/procedures for ongoing auditing of management system/operational areas).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Interviewed** selected operational managers (focus: interface with quality assurance program).
- ☐ **Examined** selected audit reports (focus: audit scope/process/organizational interface).
- ☐ **Coordinated** to verify implementation of quality assurance audit program in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Audit, Group Company and Quality Assurance.

The quality assurance program comprises two complementary functions: To monitor an operator's compliance with relevant regulations and standards, as well as to evaluate and continually improve operational safety performance. Such functions are elements of the Safety Assurance component of the SMS framework.

In some organizations the quality assurance program may have a different name (e.g. internal audit program, internal evaluation program).

In certain circumstances, an operator may have the quality assurance audit function performed by an external organization. This typically occurs when the operator is affiliated with one or more other organizations in a Group Company. However, an operator might also choose to simply outsource the quality assurance audit function to a qualified external service provider that is not part of or associated with a Group Company. In both cases, the operator, as the AOC holder, has the ultimate responsibility for ensuring the quality assurance program meets the needs of its organization in accordance with the specifications of this standard.

A robust quality assurance program ensures a scope of auditing that encompasses all areas of the organization that impact operational quality in terms of safety and/or security. Operational functions include flight operations, operational control/flight dispatch, maintenance operations, cabin operations, ground handling and cargo operations.

This provision is designed to permit flexibility in the implementation of the quality assurance program. The structure and organization of the program within an operator's management system, whether

centralized, non-centralized or a combination thereof, is at the discretion of the operator in accordance with its corporate culture and regulatory environment.

An effective audit program includes:

- Audit initiation, including scope and objectives;
- Planning and preparation, including audit plan and checklist development;
- Observation and gathering of evidence to assess documentation and implementation;
- Analysis, findings, actions;
- Reporting and audit summary;
- Follow-up and close out.

To ensure auditors gather sufficient evidence to produce realistic assessments during an audit, the program typically includes guidance that defines the various sampling techniques that are expected to be used by auditors in the evidence collection phase of the audit.

The audit process typically includes a means whereby the auditor and responsible personnel from the audited area have a comprehensive discussion and reach agreement on the findings and corresponding corrective actions. Clear procedures are established to resolve any disagreement between the auditor and audited area. All action items require follow-up to ensure closeout within an appropriate period of time.

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

ORG 2.1.2

The Operator shall appoint a manager with appropriate qualifications, authority and independence that is responsible for:

(i) The performance of the quality assurance program;

(ii) Ensuring communication and coordination with operational managers in the management of operational risk;

(iii) Dissemination of information to management and non-management operational personnel as appropriate to ensure an organizational awareness of relevant quality assurance issues and results. **(GM)**

Note: *If the Operator outsources operational functions to an external service provider, the use of the external service provider's quality assurance program manager for the purpose of conforming to the specifications of this provision shall be considered a conflict of interest, unless the Operator and the external service provider are both affiliates within the same Group Company.*

Auditor Actions

☐ **Identified** quality assurance program manager.

☐ **Examined** job description of quality assurance program manager (focus: qualifications/duties/ responsibilities).

☐ **Interviewed** quality assurance program manager.

☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Quality Assurance Manager.

The designated manager (or multiple managers if an operator does not have a centralized program) is appointed to oversee the implementation of the activities and processes associated with the quality assurance program.

The exact title of the manager(s) designated as responsible for the quality assurance program may vary depending on the organization.

Operational managers have direct responsibility for the safety and security of operations, and therefore always have the authority to develop and implement corrective action as necessary to address audit findings in their respective areas of operations.

The manager of the quality assurance program is "operationally independent" in a manner that ensures objectivity is not subject to bias due to conflicting responsibilities.

To be effective, an individual designated as manager of the quality assurance program has appropriate qualifications for the position, which may include:

- Formal training or certification as a quality auditor;
- Relevant operational and auditing experience;
- Formal training in risk management.

Quality assurance audit activities may be centrally controlled or controlled within each relevant operational function as long as independence is maintained. Typically, the manager of the quality assurance program has direct lines of communication to senior management to ensure the efficient reporting of safety and security issues, and to ensure such issues are appropriately addressed.

An effective quality assurance program includes the dissemination of appropriate information for the purpose of maintaining an ongoing awareness of quality assurance results that might affect compliance, operational safety or security or identify opportunities for improvement. As an example, such information might include a summary of audit program results such as finding, causation, risk, error trends and opportunities for continuous improvement.

The method of dissemination is commensurate with the target audience and the size of the organization. Typical means could include periodic briefings or presentations, or the issuance of magazines, newsletters or bulletins in either an electronic or paper form.

In certain circumstances, an operator may have the quality assurance audit function performed by an external organization (see guidance for ORG 2.1.1). in such cases, the operator will still ensure its quality assurance program has a manager in accordance with the specifications of this standard.

ORG 2.1.3 (Intentionally open)

ORG 2.1.4

If the Operator is on the IOSA Registry, the Operator shall ensure the quality assurance program as specified in ORG 2.1.1 provides for the auditing of the IOSA Standards and Recommended Practices (ISARPs) a minimum of once during the IOSA registration period. For internal audits of the ISARPs, the Operator shall have processes that ensure:

(i) The effective edition of the IOSA Standards Manual (ISM) is used;

(ii) Auditor Actions are accomplished by auditors;

(iii) Recording and retention of information associated with the internal audit of individual ISARPs as specified in Table 1.2. **(GM)**

Note: *If a new edition of the ISM becomes effective before the last 5 months of the Operator's IOSA registration period, the Operator shall take into account all changes that might require additional auditing (e.g. new or significantly revised ISARPs).*

Auditor Actions

☐ **Identified/Assessed** processes that ensure auditing of all ISARPs during the IOSA registration period.

☐ **Identified/Assessed** internal audit processes/procedures (focus: use of effective ISM edition; auditors accomplish Auditor Actions).

☐ **Interviewed** quality assurance program manager.

☐ **Interviewed** selected internal auditors.

☐ **Examined** selected records (database, procedural documents) of audits performed against ISARPs (focus: effective ISM edition used, all specified information included, Auditor Actions accomplished).

☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Auditor Actions, IOSA Operator, IOSA Registration Period and Registration Renewal Audit.

The currently effective edition of the ISM is used for auditing of the ISARPs during the first 19 months of the IOSA registration period. Use of an ISM edition that becomes effective in the final five (5) months of the operator's registration period is optional.

The accomplishment of Auditor Actions as specified in item (ii) is necessary to ensure internal auditors gather the necessary evidence to determine whether (or not) a standard or recommended practice is documented and implemented by the operator.

Table 1.2, as specified in item (iii), includes a note that refers to procedural documents. An example of a procedural document is an audit checklist in which all specified audit information associated with the audit of the individual ISARPs is recorded, including accomplishment of the Auditor Action steps.

IATA continues to provide a template in the form of a spreadsheet to record all required information as specified in ORG 2.1.4 and Table 1.2.

To the extent possible, auditing of the ISARPs should be spread out over the full registration period rather than waiting to conduct all auditing just prior to the registration renewal audit.

Refer to the IAH for information relevant to auditing of the ISARPs under the quality assurance program.

ORG 2.1.5

The Operator shall have an audit planning process and sufficient resources to ensure audits are:

(i) Scheduled at intervals to meet regulatory and management system requirements;

(ii) Conducted within the scheduled interval. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** quality assurance audit planning process (focus: audits planned/scheduled/conducted in accordance with applicable internal/external requirements).
- ☐ **Identified/Assessed** audit resources (focus: availability of sufficient (auditors/other resources to accomplish audit plan).
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Crosschecked** audit plan with selected audit reports (focus: audits conducted in accordance with audit plan).
- ☐ **Coordinated** to verify implementation of audit plan in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

The planning process produces a schedule of the audit modules to be conducted within the planning period (e.g. calendar year) and reflect the status of each audit module, to include the applicable audit interval (e.g. 12, 24, 36 months), the date of the previous audit and the scheduled due date for the next audit.

The planning process would typically include provisions for re-scheduling or deferral of audits in accordance with the operator's program limitations.

Refer to the IAH for information relevant to planning associated with auditing of the ISARPs.

ORG 2.1.6

The Operator shall ensure the audit planning process defines the scope of each audit, as appropriate for the area being audited, and also:

(i) Includes audit objectives that address ongoing compliance with regulatory requirements, Operator standards and other applicable regulations, rules and standards;

(ii) Considers relevant operational safety or security events that have occurred;

(iii) Considers results from previous audits, including the effectiveness of corrective action that has been implemented. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** quality assurance audit planning process (focus: audits planned/scheduled/completed in order to meet applicable internal/external requirements).
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Examined** selected audit plans (focus: audit scope/objectives defined; operational events/previous audits considered).
- ☐ **Crosschecked** audit plan with selected audit reports (focus: audits conducted in accordance with audit plan).
- ☐ **Other Actions** (Specify)

Guidance

The audit scope refers to the breadth of operational disciplines or operational areas covered by an audit and therefore will vary depending on the focus area for each audit (e.g. flight dispatch function, dangerous goods handling, ramp handling operations, line maintenance activities).

Audit objectives define tangible achievements expected to result from an audit, normally expressed as a statement of intent (e.g. to determine compliance with regulatory requirements, to establish conformity with operator standards, to assess conformity with IOSA standards, to determine efficiency of operations).

To be effective, auditors prepare for an audit of a particular area of operations by:

- Conducting research into any relevant incidents or irregularities that may have occurred;
- Reviewing reports from previous audits.

Refer to the IAH for information relevant to planning associated with auditing of the ISARPs.

ORG 2.1.7

The Operator shall have a process for addressing findings that result from audits conducted under the quality assurance program, which ensures:

(i) Identification of root cause(s);

(ii) Development of corrective action as appropriate to address findings;

(iii) Implementation of corrective action in appropriate operational area(s);

(iv) Evaluation of corrective action to determine effectiveness. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** process for addressing quality assurance audit findings.
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Examined** selected audit reports/records (focus: identification of root cause, development/implementation of corrective action, follow-up to ensure effectiveness).
- ☐ **Coordinated** to verify implementation of audit findings process in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Certain audit findings might fall under the category of hazards to operations. In such cases, the hazard would be subject to the risk assessment and mitigation process in the development of corrective action.

Refer to the IAH for information relevant to auditing under the quality assurance program.

ORG 2.1.8

The Operator shall ensure the quality assurance program uses auditors that are impartial and functionally independent from the operational activities to be audited. **(GM)**

Note: *If the Operator outsources operational functions to an external service provider and uses auditing as the process to monitor the external service provider as specified in ORG 2.2.1 and 2.2.2, the use of the external service provider's auditors to perform such auditing shall be considered a conflict of interest, unless the Operator and the external service provider are both affiliates within the same Group Company.*

Auditor Actions

- ☐ **Identified/Assessed** quality assurance auditor administration program (focus: definition of impartial/functionally independent as applied to quality assurance program auditors; policies/procedures in place that ensure auditor impartiality/functional independence).
- ☐ **Interviewed** quality assurance program manager (focus: application or policies/procedures that ensure auditor impartiality/functional independence).
- ☐ **Interviewed** selected quality assurance auditors (focus: verification of functional independence during assigned audit activities).
- ☐ **Crosschecked** selected audit reports (focus: auditors are functionally independent from the activities audited).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Group Company.

A quality assurance program is independent in a manner that permits the scheduling and conduct of audits as deemed appropriate for the size and scope of operations. Functional independence ensures auditors are not put in a position where their objectivity may be subject to bias due to conflicting responsibilities.

A code of conduct may be used to enhance the impartiality and independence of auditors. An effective auditor code of ethics would require auditors:

- To act in a strictly trustworthy and unbiased manner in relation to both the organization to which they are employed, contracted or otherwise formally engaged and any other organization involved in an audit performed by them or by personnel under their direct control;
- To disclose to their employer any relationship they may have with the organization to be audited before undertaking any audit function in respect of that organization;
- Not to accept any gift, commission, discount or any other profit from the organization audited, from their representatives, or from any other interested person nor knowingly allow personnel for whom they are responsible to do so;
- Not to disclose the findings, or any part of them, nor to disclose any other information gained in the course of the audit to any third party, unless authorized in writing by both the auditee and the audit organization, if applicable;
- Not to act in any way prejudicial to the reputation or interest of the audit organization; and
- In the event of any alleged breach of this code, to co-operate fully in any formal enquiry procedure.

An auditor may be considered functionally independent from the operational activities to be audited when he/she is not responsible for the activity being audited (at the time of the audit). For example, a flight crew member may audit line flight operations from the flight deck jump seat as an independent observer (supernumerary) but may not do so when functioning as part of the operating crew (or functioning as an augmenting crew member).

Refer to the IAH for information relevant to auditor qualification and independence.

ORG 2.1.9

The Operator shall have a training and qualification program that ensures auditors that conduct auditing under the quality assurance program as specified in ORG 2.1.1:

(i) Have the knowledge, skills and work experience needed to effectively assess areas of the management system and operations that will be audited;

(ii) Maintain an appropriate level of current audit experience;

(iii) Complete initial and continuing auditor training that provides the knowledge and understanding necessary to effectively conduct audits against:

(a) Applicable regulations and standards;

(b) If the Operator is currently on the IOSA Registry, the ISARPs.

(iv) Are evaluated on a periodic basis. **(GM)**

Note: *Sub-specification (iii) (b) is applicable only to auditors that may be assigned to conduct internal auditing against the ISARPs.*

Auditor Actions

- ☐ **Identified/Assessed** auditor training and qualification program.
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Examined** selected individual auditor records (focus: completion of initial/continuing qualification/periodic evaluations, in accordance with program standards).
- ☐ **Interviewed** selected quality assurance auditors (focus: verification of initial/continuing qualifications).
- ☐ **Crosschecked** selected audit reports/records (focus: currency of auditors).
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for the operator to have a program that ensures all auditors that conduct auditing under its quality assurance program, including internal auditor personnel (e.g. employees) or external auditor personnel (e.g. consultants), are trained, evaluated and qualified in accordance with the criteria specified in this standard.

The delivery of auditor training and evaluation under the operator's program may be accomplished by the operator or by an external party (or a combination of both) as long as all auditors that conduct auditing under the operator's quality assurance program are trained, evaluated and qualified in accordance with the criteria specified in this standard.

Internationally recognized standards published in ISO 19011 provide a reliable guide for the training and/or certification of auditors used in the quality assurance program.

For all auditors that conduct auditing of the management system, and of operations and maintenance functions for the operator under its quality assurance program as specified in ORG 2.1.1, training and qualification typically addresses the following subject areas:

- Application of audit principles, procedures and techniques;
- Planning and organizing work effectively;
- Conducting the audit within the agreed timescale;
- Prioritizing and focusing on matters of significance;
- Collecting information (i.e. audit evidence) through effective interviewing, listening, observing and examination of documents, records and data;
- Understanding the appropriateness and consequences of using sampling techniques for auditing;
- Verifying the accuracy of collected information;
- Confirming the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- Assessing those factors that can affect the reliability of the audit findings and conclusions;

- Using work documents to record audit activities;
- Preparing audit reports;
- Maintaining the confidentiality and security of information;
- Communicating effectively, either through personal linguistic skills or through an interpreter.

For those auditors assigned to conduct auditing against the ISARPs as specified in ORG 2.1.4, training and qualification typically addresses the following additional subject areas:

- IOSA program overview;
- IOSA documentation;
- Understanding the role of the ICAO annexes as the primary source of specifications contained in the ISARPs;
- Reading and understanding the ISARPs;
- IOSA quality assurance requirements (ORG subsection 2.1);
- Auditor Actions;
- Mandatory observations;
- Root cause analysis;
- Auditing ORG and repeated ORG ISARPs;
- Auditing SMS;
- Auditing quality assurance;
- Assessing outsourced operational functions.

Refer to the IAH for information relevant to the training and qualification of auditors that assess conformity with the ISARPs.

2.2 External Monitoring

ORG 2.2.1

The Operator shall have processes to monitor external service providers that conduct outsourced operational functions for the Operator to ensure requirements that affect the safety and/or security of operations are being fulfilled. **(GM)** ►

Note: *IOSA or ISAGO registration as the only means to monitor is acceptable provided the Operator obtains the latest of the applicable audit report(s) through official program channels and considers the content of such report(s).*

Auditor Actions

- ☐ **Identified/Assessed** processes for monitoring external service providers that conduct outsourced operational functions.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records/reports resulting from monitoring of service providers (focus: monitoring process ensures provider is fulfilling applicable safety/security requirements).
- ☐ **Coordinated** to verify implementation of service provider monitoring in applicable operational areas.
- ☐ **Other Actions** (Specify)

Guidance

An operator has a responsibility to ensure outsourced operational functions are conducted in a manner that meets its own operational safety and security requirements. A monitoring process is necessary to satisfy that responsibility, and such process would be applicable to any external service provider that conducts outsourced operational functions, including the parent organization or a separate affiliate of the operator.

In some regulatory jurisdictions, there may be a regulatory control process that permits certain organizations to meet rigorous standards and become approved to conduct outsourced operations or maintenance for an operator. Such regulatory control process would be an acceptable means for

meeting the specification of this provision if it can be demonstrated by the operator that the regulatory control process:

- Includes ongoing monitoring of the approved service providers;
- Such monitoring is sufficiently robust to ensure the approved service providers fulfill the operational requirements of the operator on a continuing basis.

Achieving and maintaining IOSA and/or ISAGO registration is a way for an external service provider to demonstrate fulfillment of requirements that affect the safety and/or security of operations. Thus, an operator's process that requires such service providers to maintain IOSA and/or ISAGO registration would generally be acceptable as a method of monitoring.

Using the IOSA and/or ISAGO programs to satisfy the specifications in this provision would require that an operator has access, preferably unrestricted access, to all information and data provided by the respective registration programs. Such access would be subject to receiving the relevant authorizations for individual reports. This type of monitoring would include a regular review of the registry site(s) to identify any potential annotations or restrictions that might have been placed on an operator's or provider's registration.

Using IOSA and ISAGO as described would also require an operator to request relevant audit reports through proper and official program channels. For IOSA this would require requesting an IAR through IATA and for ISAGO it would require participation in the ISAGO program. A review of the information contained in the audit report(s) would ideally complement and/or supplement any additional monitoring measures an operator is applying to ensure the service provider is fulfilling all relevant requirements. For example, combining the information from the report(s) with a risk assessment would be one option to have acceptable assurance that all requirements are fulfilled.

To ensure effective monitoring, consideration is given to a range of internal and external methods for use in the oversight of external service providers. Methods might include auditing, systematic review and risk assessment of reported hazards and/or occurrences, monitoring of performance output (KPIs), reporting and governance processes; monitoring and analysis of targeted risk areas, as well as the establishment of an effective two-way communication link with the service provider.

Under certain circumstances, operational functions may be involuntarily removed from an operator and conducted by a governmental or quasi-governmental authority that is not under the control of the operator (e.g. passenger or baggage security screening at some airports). Under such circumstances, the operator would have a process to monitor output of the function being conducted by the authority to ascertain desired results are being achieved.

If an operator is part of a Group Company and has management and/or operational functions performed by an affiliate organization that is part of the same Group Company, an operator may demonstrate monitoring of the external organization by processes that ensure functions performed by the affiliate organization for the operator are:

- Subjected to auditing under the quality assurance program of the affiliate organization;
- Continually satisfying the needs of the operator.

ORG 2.2.2

The Operator *should* include auditing as a process for the monitoring of external service providers in accordance with ORG 2.2.1. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** auditing processes used for monitoring external service providers that conduct outsourced operational functions.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records/reports resulting from auditing of service providers (focus: audit process ensures provider is fulfilling applicable safety/security requirements).
- ☐ **Coordinated** to verify implementation of service provider auditing in applicable operational areas.
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for an operator to use, as deemed appropriate for the situation, auditing as one of the processes for satisfying the requirement for monitoring external service providers (as specified in ORG 2.2.1).

Both IOSA and ISAGO are audit programs, so, where applicable, the use of IOSA or ISAGO registration could be considered as an audit process for the purpose of monitoring external service providers.

ORG 2.2.3

The Operator shall have a process that provides for the auditing of other operators that transport passengers of the Operator under a commercial aviation agreement. Such process shall ensure the following with respect to the audit of other operators:

(i) The audit is conducted against and requires conformity with applicable ICAO standards;

(ii) An initial audit is conducted prior to the commencement of the above-specified passenger transport operations;

(iii) A subsequent audit is conducted during every 24-month period following commencement of the above-specified passenger transport operations. **(GM)**

Note: *A commercial aviation agreement as specified in this standard includes the following:*

- *ACMI Lease (wet lease) Agreement*
- *Capacity Purchase Agreement (CPA)*
- *Code Share Agreement*
- *Damp Lease Agreement*

Note: *The specifications of this standard shall be applicable to the Operator if it has transported its passengers on another operator under any of the specified commercial aviation agreements during the most recent IOSA registration period.*

Note: *IOSA registration indicates an operator is in conformity with all applicable ICAO standards and thus is acceptable as the audit of another operator as specified in this provision provided the Operator obtains the latest applicable audit report(s) through official program channels and considers the content of such report(s).*

Auditor Actions

- ☐ **Identified/Assessed** process for monitoring safety/security performance of external operators that transport passengers of the Operator.
- ☐ **Interviewed** responsible managers.
- ☐ **Examined** plan/methods for monitoring applicable other operators (focus: includes all operators that transport the operator's passengers under a commercial aviation agreement).
- ☐ **Examined** selected monitoring reports of other operators (focus: monitoring process ensures the other operator is fulfilling applicable safety/security requirements).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of ACMI Lease Agreement, Capacity Purchase Agreement (CPA), Code Share Agreement, Damp Lease Agreement, IOSA Registration Period and Wet Lease Agreement.

The intent of this provision is for an operator to have a process that provides for the auditing of any other operator with which it has entered or will enter into a commercial aviation agreement to transport its passengers on flights conducted by the other operator. Such audit verifies that the other operator meets applicable ICAO standards and may be conducted either by the operator or by a third party that is acceptable to the operator.

Another operator that is on the IOSA Registry has already been audited and found to meet applicable ICAO safety standards. Therefore, conformity with this standard does not require an operator to provide for an additional audit of another operator that is on the IOSA Registry as long as such

registration is maintained by the other operator and any registration annotations have been taken into consideration by the operator.

Applicable ICAO standards as specified in item (i) are those standards contained in Annexes 1, 6, 8, 17, 18 and 19 that would be applicable to the other operator being audited.

A complete cross-reference list of ICAO-IOSA standards may be found at www.iata.org/iosa.

2.3 Product Control

ORG 2.3.1

The Operator *should* have processes to ensure equipment or other operational products relevant to the safety or security of aircraft operations that are purchased or otherwise acquired from an external vendor or supplier meet the product technical requirements specified by the Operator prior to being used in the conduct of operations or aircraft maintenance. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** processes for ensuring acquired operational products meet technical requirements.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected product acceptance records (focus: acquired products meet applicable technical requirements).
- ☐ **Coordinated** to verify product acceptance processes implemented in applicable operational areas).
- ☐ **Other Actions** (Specify)

Guidance

This provision applies only to *products* that are purchased or otherwise acquired from an external supplier or vendor. Whereas purchasing might be the most typical means of acquiring such products, other means might be also be used (e.g. lease, barter).

This provision does not apply to outsourced *operational functions* or *services* that are provided by an external organization or service provider (this is addressed in ORG 1.6.1 and 1.6.2).

This provision does not apply to electronic navigation data products used in flight (e.g. FMS database) or for operational control (e.g. flight planning database). The acquisition of such navigation data products requires control procedures, as specified in Sections 2 (FLT) and 3 (DSP).

Following are some examples of products that could have a negative effect on operations if put into service with substandard quality (i.e. the operator's technical standards are not met).

- Training devices (e.g. simulators, door mock-ups);
- Cabin safety cards or videos;
- Cabin service carts or trolleys;
- Onboard safety equipment (e.g. PBE, life jackets);
- Ground support equipment;
- Operational software, databases (non-navigation);
- Security screening equipment;
- Unit load devices (ULDs).

Part of the process is a method for identifying products that have a direct effect on the safety or security of operations.

To ensure technical specifications are met, a process may focus on the supplier, the product or a combination of both.

The process may include an evaluation of suppliers, with the selection of suppliers based on their ability to supply products in accordance with the operator's requirements and technical specifications.

The use of formal industry supplier audit or evaluation programs is one means for assessing the abilities of suppliers to deliver quality products, such as the Coordinating Agency for Supplier Evaluation (CASE).

Implementation of a rigorous receiving inspection process (or equivalent activity) provides another means of verifying that operationally critical products meet specified technical requirements prior to such products being put into service.

2.4 Data Management

ORG 2.4.1

The Operator shall have an electronic database to ensure the effective management of information and data associated with audits conducted under the quality assurance program as specified in ORG 2.1.1 and ORG 2.1.4. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** electronic database for management of quality assurance audit data.
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Examined** selected database records (focus: content includes information/data specified in ORG 2.1.4 and Table 1.2).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Database.

A database would typically include, as a minimum, the following information associated with each audit:

- Details of each planned and conducted audit
  - Area/entity audited;
  - Status of the audit (planned, conducted, re-scheduled, completed);
  - Date of audit;
  - Objective, scope and criteria;
  - Auditor name.
- Non-conformity details:
  - Root cause(s);
  - Corrective action(s) implemented;
  - Assignment of responsibility;
  - Closure and acceptance details.

ORG 2.4.2

The Operator *should* have an electronic database to ensure effective management of data derived from the hazard identification and risk assessment and mitigation programs. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** flight safety analysis program database.
- ☐ **Interviewed** flight safety analysis program manager.
- ☐ **Observed** demonstration of flight safety analysis program database functionality.
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for an operator to have an electronic database that permits an operator to manage information and data associated with aircraft operations in a manner that results in the identification of hazards and the provision of information to operational managers as specified in ORG 3.1.1.

The type and complexity of such database will vary according to the size and scope of the organization.

ORG 2.4.3

The Operator *should* have a process to ensure reports of safety and security occurrences are submitted to IATA for inclusion in the Incident Data Exchange (IDX). Such reports *should* be submitted in accordance with the formal IDX reporting process and include incidents and reports from:

(i) Flight operations;
(ii) Cabin operations;
(iii) Ground handling operations;
(iv) Engineering and Maintenance. **(GM)**

Auditor Actions

☐ **Identified/Assessed** process for reporting incidents to IATA for inclusion in IDX.
☐ **Interviewed** responsible manager(s).
☐ **Examined** the agreement between the Operator and IATA for participation in IDX.
☐ **Examined** selected reports submitted to IATA.
☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of IATA Incident Data Exchange (IDX).

The IATA IDX is a quality source of defensible data to support analyses and production of performance and benchmarking indicators for use in the management of all operations, to include flight operations, cabin operations, and ground handling operations.

Reports submitted to IDX will be assembled and integrated in a manner that permits, through statistical analysis, the identification of trends and contributing factors associated with safety and security events.

IDX participants that regularly submit reports benefit by gaining access to the aforementioned analytical results Failure to submit reports will result in participants being excluded from the program.

The assurance of data quality and overall database integrity requires data to be submitted by participants in a uniform and consistent manner. Therefore, IDX will require a strict reporting taxonomy, including associated definitions and assumptions.

Reporting guidelines and other information can be found online at the IATA Global Aviation Data Management page (https://www.iata.org/en/services/statistics/gadm/).

☐ **ORG 2.4.4**

The Operator *should* participate in and supply data to an aggregated Flight Data Sharing Program that is applied to aircraft in its fleet with a certified take-off mass in excess of 20,000 kg (44,092 lbs). As a minimum, such program should:

(i) Have a signed agreement with the program participants (member airlines) on how their data will be utilized;
(ii) Provide a means for participants to securely transfer their flight data;
(iii) Be non-punitive and offer adequate safeguards for the de-identification of all data received from participants;
(iv) Disseminate de-identified information to participants on emerging trends and areas of interest to global aviation safety;
(v) Not use data for the purposes of investigation of the performance of individual participants.

Auditor Actions

☐ **Identified/Assessed** process for the secure transfer of data.
☐ **Interviewed** responsible manager(s).

- ☐ **Examined** the agreement between the Operator and participating operators on how the data would be utilized.
- ☐ **Examined** selected de-identified reports.
- ☐ **Other Actions** (Specify)

Guidance

Acceptable flight data sharing programs include, but are not limited to the IATA Flight Data Exchange (FDX) or any State-run, aggregated data sharing programs such as ASIAS, Data 4 Safety etc.

An aggregated flight data sharing program is a de-identified database of flight data collected from multiple participants and processed for the purposes of improvement of aviation safety through the identification of areas of safety concern and risk. Such programs also enable participants undertake comparative analysis on global or regional specific performance.

A state-run aggregated flight data sharing program is one undertaken by a competent aviation state body in a specific country e.g. The Federal Aviation Administration (FAA), European Aviation Safety Agency (EASA).

2.5 Documentation System

△ **ORG 2.5.1**

The Operator shall have a system for the management and control of documentation and/or data used directly in the conduct or support of operations. Such system shall ensure documentation:

(i) Meets all required elements specified in Table 1.1;

(ii) Contains legible and accurate information;

(iii) Is presented in a format appropriate for use in operations. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** system(s) for management/control of content/format of operational documentation/data used in operational control system.
- ☐ **Interviewed** responsible operational control manager(s).
- ☐ **Examined** selected parts of the OM (focus: legibility/accuracy/format; approval as applicable).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Documentation, Electronic Documentation and Paper Documentation.

The primary purpose of document control is to ensure necessary, accurate and up-to-date documents are available to those personnel required to use them, to include, in the case of outsourced operational functions, employees of external service providers.

Examples of documents that are controlled include, but are not limited to, operations manuals, checklists, quality manuals, training manuals, process standards, policy manuals, and standard operating procedures.

Documentation received from external sources would include manuals and other types of relevant documents that contain material that is pertinent to the safety of operations conducted by the operator (e.g. regulations, operating standards, technical information and data).

An electronic system of document management and control is an acceptable means of conformance. Within such a system, document files are typically created, maintained, identified, revised, distributed, accessed, presented, retained and/or deleted using computer systems (e.g. a web-based system). Some systems specify immediate obsolescence for any information or data that is downloaded or otherwise extracted (e.g. printed on paper) from the electronic files.

Document control might include:

- Retention of a master copy;
- Examination and approval prior to issue;
- Review and update, to include an approval process;
- Version control (electronic documents);
- Identification of revision status;
- Identification and retention of revisions as history;
- Identification and retention of background or source references as history;
- Distribution to ensure appropriate availability at points of use;
- Checking of documents to verify they remain legible and readily identifiable;
- As required, identification, update, distribution and retention of documents of external origin;
- As applicable, identification and retention of obsolete documents;
- As applicable, disposal of documents.

Additionally, control of operational manuals might include:

- Assignment of an individual with responsibility for approval for contents;
- A title page that generally identifies the operational applicability and functionality;
- A table of contents that identifies parts and sub-parts;
- A preface or introduction outlining the general contents of the manual;
- Reference numbers for the content of the manual;
- A defined distribution method and identification of recipients;
- Identification of responsibility for authorizing the manual;
- A record of revisions, both temporary and permanent;
- A list of effective pages within the manual;
- Identification of revised content.

Each “loose” documented procedure that is not held within a manual typically includes:

- A title page that identifies the operational applicability and functionality;
- Identification of the date(s) of issue and date of effectiveness;
- Reference numbers for the content;
- A distribution list;
- Identification of responsibility for authorizing the document.

△ **ORG 2.5.2** (Intentionally open)

ORG 2.5.3

The Operator *should* have a documentation system that ensures operations, maintenance and security manuals are centrally managed or coordinated under a corporate scheme of document hierarchy. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** central system for management/control of content/format of operational documentation/data (focus: common standards for documentation/data control in all areas of operations).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Examined/Compared** selected operational documents (focus: standardized documents consistent with central system standards).
- ☐ **Other Actions** (Specify)

Guidance

A centrally controlled or coordinated system ensures a standardized documentation product throughout the organization. Ideally, all documents conform to a corporate standard, thus ensuring an organization-wide consistency in documentation philosophy, format and presentation of content.

ORG 2.5.4

The Operator shall have SMS documentation, including a manual, that describes:

(i) The safety policy and objectives;

(ii) SMS requirements;

(iii) SMS processes and procedures;

(iv) Accountability, authorities and responsibilities for SMS processes and procedures. **[SMS] (GM)**

Note: *An SMS manual may be in the form of a stand-alone document or may be integrated with other organizational documents (or documentation) maintained by the Operator.*

Auditor Actions

- ☐ **Identified/Assessed** SMS documentation (focus: description of overall organizational management of safety).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected parts of SMS documentation (focus: content includes safety policy/objectives; describes/defines accountability/responsibilities for safety processes/procedures in all areas of operations).
- ☐ **Coordinated** to verify SMS documentation in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

SMS documentation is an element of the Safety Policy and Objectives component of the SMS framework.

SMS documentation is typically scaled to the size and complexity of the organization and describes both the corporate and operational areas of safety management to show continuity of the SMS throughout the organization. Typical documentation would include a description of management positions and associated accountability, authorities, and responsibilities within the SMS.

To ensure personnel throughout the organization are informed, SMS documentation includes a description of the operator's approach to safety management. Such descriptive information would be contained in a manual and presented in a manner that ensures the SMS information is clearly identifiable. The exact title and structure of such manual may vary with each operator.

Depending on the size, structure and scope of an operator's organization, as well as the complexity of its operations, SMS documentation may be in the form of stand-alone documents or may be integrated into other organizational documents.

Requirements for SMS documentation will vary according to the individual state safety program (SSP).

SMS documentation typically addresses:

- Scope of the SMS;
- Safety policy and objectives;
- Safety accountability;
- Key safety personnel;
- Documentation control procedures;
- Coordination of emergency response planning;
- Hazard identification and risk management schemes;
- Safety assurance;
- Safety performance monitoring;

- Safety auditing (safety and quality auditing may be combined);
- Management of change;
- Safety promotion;
- Outsourced services.

Expanded guidance may be found in the ICAO SMM, Document 9859.

2.6 Records System

ORG 2.6.1

The Operator shall have a system for the management and control of operational records to ensure the content and retention of such records is in accordance with requirements of the Authority, as applicable, and to ensure operational records are subjected to standardized processes for:

(i) Identification;
(ii) Legibility;
(iii) Maintenance;
(iv) Retrieval;
(v) Protection, integrity and security;
(vi) Disposal, deletion (electronic records) and archiving. **(GM)** ►

Note: *The operational records system specified in this standard shall also include the management and control of SMS operational records.*

Auditor Actions

☐ **Identified/Assessed** system for management/control of operational records (focus: system includes standardized processes as specified in standard).
☐ **Interviewed** responsible management representative(s).
☐ **Examined** selected examples of operational records.
☐ **Coordinated** to verify implementation of records management/control processes in all operational areas.
☐ **Other Actions** (Specify)

Guidance

The system addresses the management and control of all records associated with operations, which includes personnel training records, and also includes any other records that document the fulfillment of operational requirements (e.g. aircraft maintenance, operational control, operational security).

SMS operational records substantiate the ongoing operation of the operator's SMS and may be managed and controlled within either a centralized or standalone records system. SMS operational records typically include or provide a record of the following:

- Hazards register and hazard/safety reports;
- SPIs, SPTs and related charts;
- Completed safety risk assessments;
- SMS internal reviews or audits;
- SMS/safety training;
- SMS/safety committee meeting minutes.

ORG 2.6.2

If the Operator uses an electronic system for the management and control of records, the Operator shall ensure the system provides for a scheduled generation of backup record files. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** process for scheduled backup of electronic operational records (focus: system defines schedule for periodic file backup).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Coordinated** to verify applicable backup process is implemented in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Maintaining records in electronic files is a reliable and efficient means of short and long-term storage. The integrity of this type of record-keeping system is ensured through secure, safe storage and backup systems.

In an electronic records system, record files are managed and controlled (i.e. created, maintained, identified, updated, accessed, retained and deleted) using computer systems, programs and displays (e.g. a web-based system).

To preclude the loss of records due to hardware or software failures, an electronic system is programmed to create backup files on a schedule that ensures records are never lost. Typically, an electronic system provides for file backup on a daily basis.

Where necessary, the look and feel of electronic records is similar to that of a paper record.

The retention period for records is defined by the operator and, if applicable, will always be in accordance with requirements of the Authority.

Hardware and software, when updated or replaced, is retained to enable retrieval of old records.

3 Risk Management

3.1 Hazard Identification

ORG 3.1.1

The Operator shall have a hazard identification program that is implemented and integrated throughout the organization and includes a combination of reactive and proactive methods of hazard identification. **[SMS] (GM)** ►

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** organizational safety hazard identification program (focus: program identifies hazards to aircraft operations; describes/defines method(s) of safety data collection/analysis).
- ☐ **Identified/Assessed** cross-discipline process for safety hazard identification (focus: all operational disciplines participate in process).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected records/documents that illustrate organizational integration (focus: coordinated involvement of all operational disciplines in hazard identification process).
- ☐ **Examined** selected examples of hazards identified through data collection/analysis.
- ☐ **Coordinated** to verify implementation of safety hazard identification program in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Hazard (Aircraft Operations) and Safety Risk.

Hazard identification is an element of the Safety Risk Management component of the SMS framework.

The methods used to identify hazards will typically depend on the resources and constraints of each particular organization. Some organizations might deploy comprehensive, technology-intensive hazard identification processes, while organizations with smaller, less complex operations might implement more modest hazard identification processes. Regardless of organizational size or complexity, to ensure all hazards are identified to the extent possible, hazard identification processes are necessarily formalized, coordinated and consistently applied on an on-going basis in all areas of the organization where there is a potential for hazards that could affect aircraft operations.

To be effective, reactive and proactive processes are used to acquire information and data, which are then analyzed to identify existing or predict future (i.e. potential) hazards to aircraft operations.

△ Examples of processes that typically yield information or data for hazard identification are shown in the list below. The most common type of process associated with each example is shown in parentheses, although some could be used both:

- Confidential or other reporting by personnel (proactive);
- Investigation of accidents, incidents, irregularities and other non-normal events (reactive);
- Flight data analysis (proactive);
- Observation of flight crew performance in line operations and training (proactive);
- Quality assurance and/or safety auditing (proactive);
- Safety information gathering or exchange (external sources).

Processes would be designed to identify hazards that might be associated with organizational business changes (e.g. addition of new routes or destinations, acquisition of new aircraft type(s), the introduction of significant outsourcing of operational functions).

Typically, hazards are assigned a tracking number and recorded in a log or database. Each log or database entry would normally include a description of the hazard, as well as other information necessary to track associated risk assessment and mitigation activities.

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 3.1.2

The Operator shall have an operational safety reporting system that is implemented throughout the organization in a manner that:

(i) Encourages and facilitates personnel to submit reports that identify safety hazards, expose safety deficiencies and raise safety concerns;

(ii) Ensures mandatory reporting in accordance with applicable regulations;

(iii) Includes analysis and management action as necessary to address safety issues identified through the reporting system. **[SMS] (GM)** ►

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** organizational operational safety reporting system (focus: system urges/facilitates reporting of hazards/safety concerns; includes analysis/action to validate/address reported hazards/safety concerns).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** records of selected operational/safety reports (focus: analysis/follow-up to identify/address reported hazards/safety concerns).
- ☐ **Coordinated** to verify implementation of operational safety reporting system in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Safety reporting is a key aspect of SMS hazard identification and risk management.

Frontline personnel, such as flight or cabin crew members and maintenance technicians, are exposed to hazards and face challenging situations as part of their everyday activities. An operational reporting system provides such personnel with a means to report these hazards or any other safety concerns so they may be brought to the attention of relevant managers.

To build confidence in the reporting process and encourage more reporting, an acknowledgement of receipt is typically provided to each person that submits a report.

An effective system provides for a review and analysis of each report to determine whether a real safety issue exists, and if so, ensure development and implementation of appropriate action by responsible management to correct the situation.

Refer to ORG 1.2.2, which specifies a corporate safety reporting policy and addresses the importance of having an effective reporting culture to ensure the proactive identification of potential safety deficiencies.

Refer to the IAH for information that identifies repeats of this provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 3.1.3

The Operator *should* have a confidential safety reporting system that is implemented throughout the organization in a manner that encourages and facilitates the reporting of events, hazards and/or concerns resulting from or associated with human performance in operations. **(GM)** ►

Auditor Actions

- ☐ **Identified/Assessed** organizational confidential safety reporting system (focus: system urges/facilitates reporting of events/hazards/safety concerns caused by humans; reporters are assured confidentiality; includes analysis/action to validate/address reported hazards/safety concerns).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Examined** records of selected confidential safety reports (focus: assurance of confidentiality, analysis/follow-up to identify/address reported hazards/safety concerns).
- ☐ **Crosschecked** to verify implementation of confidential safety reporting system in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

The specified confidential safety reporting system is sometimes referred to as a Confidential Human Factors (or Incident) Reporting System.

The success of a confidential safety reporting system depends on two fundamentals:

- The ability of the organization to assure absolute protection of a report submitted by any individual;
- The level to which individuals within the organization exercise their freedom to report actual or potential unsafe conditions or occurrences.

In certain states, information submitted under a pledge of confidentiality could be subject to laws protecting such information. Therefore, an operator would typically have procedures in place to protect report confidentiality (e.g. de-identification).

There is a difference between confidential reporting and anonymous reporting. Confidential reporting is the preferred system because it permits feedback to the reporter in response to the report. Not only is the reporter entitled to an explanation, but also such feedback provides excellent incentive for the submission of future reports.

The effectiveness of a confidential safety reporting system is determined by a basic requirement for safeguarding safety and risk information. Typically, individuals will continue to provide information only when there is confidence that such information will be used only for safety purposes and will never be compromised or used against them.

An effective confidential safety reporting system might typically include:

- A process that provides absolute protection of confidentiality;
- An articulated policy that encourages reporting of hazards and human errors in operations;
- A shared responsibility between the individual flight and cabin crew members (or, if applicable, respective professional associations) and the organization to promote a confidential safety reporting system;
- A tracking process of action taken in response to reports;
- A process to provide feedback to the reporter;
- A communication process for ensuring flight and cabin crew members, as well as other relevant personnel, are informed of potential operating hazards through dissemination of de-identified report information.

ORG 3.1.4

The Operator *should* have a program for the systematic acquisition and analysis of data from observations of flight crew performance during normal line operations. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** line operations monitoring program (focus: observations of flight crew performance on routine line flights; trained/qualified non-evaluation observers; acquisition/analysis of data from observations of identification of operational threats/errors/risk; production of data/recommendations used to mitigate risk).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Interviewed** line operations observer(s) and data analyst(s).
- ☐ **Examined** selected line monitoring program reports (focus: analysis of observation data; identification of flight safety hazards; recommendations to mitigate risk).
- ☐ **Other Actions** (Specify)

Guidance

If implemented, line monitoring would be considered a *proactive* hazard identification activity in an SMS.

A line operations monitoring program is a completely different activity from line evaluation (or line checking) of the flight crew. Line operations monitoring cannot be accomplished in conjunction with any type of operational evaluation of the flight crew.

Under this program, flight crew performance in a normal line environment is observed from the flight deck jump seat by individuals who have been specially selected and trained. Observers, with the cooperation of the flight crew, systematically gather operational data that can be analyzed and used to make real improvements to certain areas of the operation. Observers are particularly aware of, and record, threats and errors that occur in the operating environment.

The Line Operations Safety Audit (LOSA) is a well-known and successful example of a normal line operations monitoring program.

An acceptable program would have the following characteristics:

- A planned and organized series of observations of flight crew performance during normal line flights is typically conducted a minimum of once during every four-year period.
- Observations are conducted on regular and routine line flights, and the flight crew is advised and clearly understands that normal line monitoring is not an evaluating, training or checking activity. The flight crew would be expected to operate as if the observer were not there.
- There is mutual support and cooperation from both the management of the operator and flight crew members (through their professional association, if applicable).
- Participation from the flight crew is voluntary; observations are not conducted unless permission is received from the flight crew.

- Data collected from observations are confidential, de-identified and used for safety enhancement purposes only. Data from an observation are never permitted to be used for disciplinary action unless there is evidence of willful misconduct or illegal activity.
- Procedures are in place to ensure data from observations are retained in a way that ensures effective security.
- Objectives of observations are clearly defined, and collected data are always used to address specific issues that affect flight safety.
- Observers are specifically selected and trained (calibrated) to ensure a high level of consistency and standardization in the data being collected. Observers are objective, impartial and have a high level of integrity.
- There is a process in place to ensure data collected from observations are subjected to analysis from appropriately diverse subject matter experts to ensure consistency and accuracy.
- Data derived from observations are analyzed and presented in a manner that identifies potential weakness and permits the operator to develop appropriate action(s) that will enhance specific aspects of the operation.
- Results from the monitoring program, including the corrective action plan, are communicated to flight crew members.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 3.1.5

The Operator shall have a process to identify changes within or external to the organization that have the potential to affect the level of safety risks associated with aircraft operations, and to manage risks that may arise from or are affected by such changes in accordance with ORG 3.1.1 and ORG 3.2.1.
[SMS] [Eff] (GM)

Assessment Tool

Desired Outcome

• The safety risks associated with aircraft operations that may arise or are affected by external or internal changes are managed and controlled to ensure they remain at an acceptable level.

Suitability Criteria (Suitable to the size, complexity and nature of operations)

• Number and type of analyzed changes.

• Means used for recording changes.

• Level of awareness within the organization.

• Data and source of information used to identify the changes that may impact the safety of aircraft operations.

Effectiveness Criteria

(i) Clear criteria are established, that define when a formal change management process must be applied

(ii) Process is applied prior to any change that has the potential to affect the level of safety risks.

(iii) All areas within the organization are aware of the process and apply it for all relevant changes.

(iv) All relevant personnel are adequately trained in the execution of the process.

(v) All changes are documented and decisions on the application of the process are recorded.

(vi) The hazard identification process involves personnel from all relevant areas within the organization.

(vii) Information is fed into the RA and mitigation process.

Auditor Actions

- ☐ **Identified/Assessed** organizational change management process (focus: process identifies/assesses internal/external changes to determine operational safety risk).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected records/documents that show processing of internal/external changes (focus: assessment of changes to determine safety risk; actions taken to implement/revise new/existing risk controls).
- ☐ **Coordinated** to verify implementation of change management process in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Change Management.

Change management is an element of the Safety Assurance component of the SMS framework and is considered a proactive hazard identification activity in an SMS.

Safety risk management requires an operator to have a formal process to identify hazards that may affect aircraft operations. Hazards may exist in ongoing aircraft operations or be inadvertently introduced whenever internal or external changes occur that could affect aircraft operations. In such cases, hazard identification as specified in ORG 3.1.1 and safety risk assessment and mitigation as specified in ORG 3.1.2 (both are repeated in other ISM sections) are integral elements of an operator's change management process.

A change management process is normally designed to ensure risk management is applied to any internal or external change that has the potential to affect an operator's established operational processes, procedures, products, equipment and services. The change management process typically takes into account the following three considerations:

- *Criticality.* Criticality assessments determine the systems, equipment or activities that are essential to the safe operation of aircraft. While criticality is normally assessed during the system design process, it is also relevant during a situation of change. Systems, equipment and activities that have higher safety criticality are reviewed following change to make sure that corrective actions can be taken to control potentially emerging safety risks.
- *Stability of systems and operational environments.* Changes might be planned and under the direct control of the operator. Examples of such changes include organizational growth or contraction, the expansion of products or services delivered, or the introduction of new technologies. Changes might also be unplanned and external to the operator, such as changing economic cycles, labor unrest and changes to the political, regulatory or operating environments.
- *Past performance.* Past performance of critical systems and trend analyses in the safety assurance process is typically employed to anticipate and monitor safety performance under situations of change. The monitoring of past performance will also assure the effectiveness of corrective actions taken to address safety deficiencies identified as a result of audits, evaluations, investigations or reports.

Expanded guidance may be found in the ICAO SMM, Document 9859.

3.2 Risk Assessment and Mitigation

ORG 3.2.1

The Operator shall have a safety risk assessment and mitigation program that includes processes implemented and integrated throughout the organization to ensure:

(i) Hazards are analyzed to determine corresponding safety risks to aircraft operations;

(ii) Safety risks are assessed to determine the requirement for risk mitigation action(s);

(iii) When required, risk mitigation actions are developed and implemented in operations. **[SMS] [Eff] (GM) ►**

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Assessment Tool

Desired Outcome

• The Operator maintains an overview of its operational risks and through implementation of mitigation actions, as applicable, ensures risks are at an acceptable level.

Suitability Criteria (Suitable to the size, complexity and nature of operations)

• Number and type of analyzed hazards and corresponding risks.

• Means used for recording risks and mitigation (control) actions.

• Safety data used for the identification of hazards.

Effectiveness Criteria

(i) Risk register(s) across the organization capture risk assessment information, risk mitigation (control) and monitoring actions.

(ii) Safety risks are expressed in at least the following components:
- Likelihood of an occurrence.
- Severity of the consequence of an occurrence.
- Likelihood and severity have clear criteria assigned.

(iii) A matrix defines safety risk tolerability to ensure standardization and consistency in the risk assessment process, which is based on clear criteria.

(iv) All relevant hazards are analyzed for corresponding safety risks.

(v) Risk mitigation (control) actions include timelines, allocation of responsibilities and risk control strategies (e.g. hazard elimination, risk avoidance, risk acceptance, risk mitigation).

(vi) Mitigation (control) actions are implemented to reduce the risk to a level of “as low as reasonably practical”.

(vii) Identified risks and mitigation actions are regularly reviewed for accuracy and relevance.

(viii) Effectiveness of risk mitigation (control) actions are monitored at least yearly.

(ix) Personnel performing risk assessments are appropriately trained in accordance with ORG 4.3.1.

(x) The program takes into consideration any area of the organization where there is a potential for hazards that could affect aircraft operations.

(xi) The program has some form of central coordination to ensure all existing or potential hazards that have been identified as relevant are subjected to risk assessment and, if applicable, mitigation.

Auditor Actions

- ☐ **Identified/Assessed** organizational safety risk assessment/mitigation program (focus: hazards analyzed to identify/define risk; risk assessed to determine appropriate action; action implemented/monitored to mitigate risk).
- ☐ **Identified/Assessed** cross-discipline process for risk assessment/mitigation (focus: all operational disciplines participate in process).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected records/documents that illustrate organizational integration (focus: coordinated involvement of all operational disciplines in risk assessment/mitigation program).
- ☐ **Examined** selected examples of risk assessment/risk mitigation action(s).
- ☐ **Coordinated** to verify implementation of safety risk assessment/mitigation in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Risk Register, Safety Risk, Safety Risk Assessment (SRA), Safety Risk Management and Safety Risk Mitigation.

Risk assessment and mitigation is an element of the Safety Risk Management component of the SMS framework.

To be completely effective, a risk assessment and mitigation program would typically be implemented in a manner that:

- Is active in all areas of the organization where there is a potential for hazards that could affect aircraft operations;
- Has some form of central coordination to ensure all existing or potential hazards that have been identified are subjected to risk assessment and, if applicable, mitigation.

The safety risks associated with an identified existing or potential hazard are assessed in the context of the potentially damaging consequences related to the hazard. Safety risks are generally expressed in two components:

- Likelihood of an occurrence;
- Severity of the consequence of an occurrence.

Typically, matrices that quantify safety risk acceptance levels are developed to ensure standardization and consistency in the risk assessment process. Separate matrices with different risk acceptance criteria are sometimes used to address long-term versus short-term operations.

A risk register is often employed for the purpose of documenting risk assessment information and monitoring risk mitigation (control) actions.

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 3.2.2

The Operator *should* have a process for safety data analysis with the purpose of predicting future risks associated with hazards to aircraft operations. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** organizational safety risk assessment/mitigation program (focus: process for analysis of safety data to predict future risks).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected results of data analysis performed to predict future risks.
- ☐ **Examined** examples of action(s) taken to address future risks identified from safety data analysis.
- ☐ **Other Actions** (Specify)

Guidance

The analysis of safety data could include probability or predictive analytical methods whereby information is extracted from historical and current data and then used to predict trends and behaviour patterns. Patterns found in historical data can help identify emerging risks and opportunities. Whereas the unknown event of interest is in the future, predictive analysis can be applied to any type of unknown in the past, present or future. The core of predictive analysis relies on capturing relationships between variables from past occurrences and exploiting them to predict the unknown outcome. If electronic systems are used, they may allow users to model different scenarios of risks or opportunities with different outcomes. This enables decision makers to assess the decisions they can make in the face of different unknown circumstances and to evaluate how they can effectively allocate limited resources to areas where the highest risks or best opportunities exist.

3.3 Flight Data Analysis (FDA)

ORG 3.3.1

If the Operator conducts flights with aircraft that have a maximum certified takeoff mass in excess of 27,000 kg (59,525 lb), the Operator shall have a flight data analysis (FDA) program that requires a systematic download and analysis of electronically recorded flight data from applicable aircraft in its fleet. The FDA program shall be non-punitive and be integrated in the Operator's SMS. **[SMS] (GM)**

Note: *Conformity with this provision is possible only when the Operator is also in conformity with ORG 3.3.3, 3.3.4 and 3.3.5.*

Auditor Actions

- ☐ **Identified/Assessed** FDA program (focus: program is non-punitive and is applied to aircraft in the fleet with a MCTOM greater than 27 000 kg).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Interviewed** FDA program manager.
- ☐ **Assessed** processes/systems for download of electronically recorded flight data (focus: usable program data is downloaded from all applicable aircraft types in the operator's fleet).
- ☐ **Assessed** status of conformity with ORG 3.3.3, 3.3.4 and 3.3.5.
- ☐ **Observed** FDA program resources and activities.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Flight Data Analysis (FDA) Program.

The FDA program fits into the Safety Assurance (safety performance monitoring/measuring) and Safety Risk Management (hazard identification) components of the SMS framework.

A systematic download and analysis of electronically recorded aircraft flight data would typically include:

- Systems on applicable aircraft that:
  - Capture flight data and permit rapid download through use of an optical disc/PC or equivalent, or
  - Capture and automatically transmit encrypted aircraft data through a ground link to a ground station.
- A ground system that transforms raw digital flight data into a usable form of information that can then be verified, processed and categorized for analysis;
- One or more ground stations (usually a desk top computer loaded with the appropriate software) to permit the analysis of flight data to identify deviations from expected performance;
- A secure database that protects and permits retention, retrieval and use of program data (e.g. data mining, research, event development).

In addition to the above, an FDA program might include optional flight animation software that provides a visual simulation of actual flight events.

The practice of analyzing recorded data from routine flight operations is a cornerstone in support of an operator's accident prevention programs. Rather than reacting to serious incidents, an effective FDA program enables a proactive identification of safety hazards associated with flight operations.

An FDA program is also used for:

- Routine flight operational measurements;
- Incident investigations;
- As applicable, continuing airworthiness.

A key element in developing an FDA program is gaining the support of flight crew members. Such support is typically achieved through a policy and/or procedures and a formal agreement that lays out the conditions for ensuring the program is non-punitive and downloaded flight data is de-identified and secure. If applicable, such policy and/or procedures would typically be set forth in a formal agreement with the association that represents flight crew members.

It is important that the FDA program clearly defines the meaning of a non-punitive environment and that relevant program participants, particularly flight crew members:

- Have a clear understanding of the types of operational behaviors that are unacceptable, and the conditions under which disciplinary action would or would not apply.

- Are provided with enough information about the process to ensure a perception of fair treatment in accordance with program policy and procedures.
- Have confidence that non-punitive principles will be applied in the treatment of events identified under the FDA program.

An effective FDA program typically includes assurance that:

- Flight data and other relevant information are analyzed thoroughly such that, as far as reasonably practicable, all relevant factors associated with an event are identified, not just the action or inaction of specific individuals.
- Investigation of FDA events focuses on systemic issues that might influence behaviors, rather than on individual actions.
- Individuals involved in the investigation of an event will be treated fairly based on the quality of their behavioral choices.
- Factual details of an event are provided to relevant operational managers for an objective review of all factors involved.

All or certain specific elements of the FDA program might be outsourced to an external service provider; however, the operator would retain overall responsibility for the maintenance of the program.

The most comprehensive approach to flight data analysis would include not only the systematic download and analysis of recorded aircraft flight data, but also acquisition, correlation and analysis of other information derived from operational safety reports, regulatory authorities, investigative bodies, OEMs and other operators.

Further guidance may be found in the following source documents:

- ICAO Doc 9859, Safety Management Manual, and ICAO Doc 10000, Manual on Flight Data Analysis Programmes (FDAP).
- CASA CAAP SMS-4(0), Guidance on the establishment of a Flight Data Analysis Program (FDAP)–Safety Management Systems (SMS).
- FAA Advisory Circular AC No: 120-82, Flight Operational Quality Assurance.
- UK CAA CAP 739, Flight Data Monitoring.

Refer to ORG 3.3.5, which addresses the integration of the FDA program in an operator's SMS.

ORG 3.3.2

The Operator *should* have a flight data analysis (FDA) program in accordance with ORG 3.3.1 that is applied to aircraft in its fleet with a certified takeoff mass in excess of 20 000 kg (44,092 lb). **(GM)**

Auditor Actions

☐ **Identified/Assessed** FDA program (focus: program is non-punitive and is applied to aircraft in fleet with MCTOM greater than 20 000 kg).

☐ **Interviewed** SMS manager and/or designated management representative(s).

☐ **Interviewed** FDA program manager.

☐ Assessed processes/systems for download of electronically recorded flight data (focus: usable data are downloaded from all applicable aircraft types in the operator's fleet).

☐ **Other Actions** (Specify)

Guidance

An FDA program for aircraft with a certified takeoff mass in excess of 20 000 kg (44,092 lb) but less than 27,000 kg (59,525 lb), will typically contain processes and procedures as specified in ORG 3.3.3, 3.3.4 and 3.3.5.

ORG 3.3.3

If the Operator has an FDA program in accordance with ORG 3.3.1, the Operator shall ensure such program has processes for:

(i) Interpretation and analysis of flight and aircraft technical data;

(ii) Flight crew liaison, including permission and responsibility for confidential discussions with flight crew members involved in events highlighted by FDA;

(iii) Data collection that comprises data that are representative of all aircraft operations for each applicable fleet type;

(iv) Dissemination of de-identified information to relevant operational personnel;

(v) Training and qualification of personnel as appropriate to perform assigned program functions. **(GM)**

Auditor Actions

- ☐ **Identified** FDA program processes (focus: program includes all required processes).
- ☐ **Interviewed** FDA program manager.
- ☐ **Examined** FDA program job descriptions (focus: tasks/qualifications appropriate for program functions performed).
- ☐ **Assessed** processes for interpretation/analysis of flight/aircraft technical data (focus: data format and qualifications of personnel appropriate for interpretation/analysis of FDA data).
- ☐ **Identified flight crew liaison process.**
- ☐ **Assessed** data collection process(es) (focus: data collected is representative of all applicable aircraft operations).
- ☐ **Examined** selected records that reflect FDA data dissemination.
- ☐ **Assessed** training and qualification processes (focus: personnel are appropriately trained and qualified for program functions performed).
- ☐ **Other Actions** (Specify)

Guidance

Responsibilities within FDA program processes may be shared among individuals based on the size and complexity of an operator's organization.

FDA program processes may be outsourced to external service providers, but the operator is always responsible for the performance of the program.

The intent of items (i) and (ii) is that functions in program processes are performed by personnel that have experience, skills and/or capabilities appropriate for the function(s) performed:

Personnel that provide interpretation and analysis of flight technical data are typically flight crew members that have an in-depth understanding of the operator's aircraft types, operating procedures, routes and airports.

Personnel that provide interpretation and analysis of aircraft technical data typically have maintenance engineering and/or appropriated maintenance technical experience and are familiar with the operator's power plant/structures/systems departments, information sources/requirements and engineering monitoring programs.

Personnel that perform flight crew liaison (i.e. the "gatekeeper" function) would typically have integrity, good judgement and the trust of both flight crew members and company management.

The intent of item (v) is a training and qualification program that ensures personnel are competent to perform assigned duties and functions within the FDA program. Personnel would typically complete initial training prior to the performance of any program functions and subsequent recurrent training to ensure continued competency.

Refer to ORG 3.3.4, which addresses the management and protection of program data and information.

ORG 3.3.4

If the Operator has an FDA program in accordance with ORG 3.3.1, the Operator shall have standards for the management and protection of program data and information that define:

(i) Methods for ensuring the integrity and validity of downloaded flight data;

(ii) Policies and procedures for data de-identification and confidentiality;

(iii) Methods for maintaining and presenting event and exceedance information for trend analysis;

(iv) Policies and procedures for data retention, retrieval and archiving;

(v) Processes for assessing and improving data management policies, methods and procedures. **(GM)**.

Auditor Actions

- ☐ **Assessed** FDA program data management/protection (focus: program standards define all aspects of management and protection of data).
- ☐ **Interviewed** FDA program manager.
- ☐ **Examined** selected records/examples of data management/protection (focus: policies/methods/procedures consistent with program standards for ensuring effective data management/protection).
- ☐ **Other Actions** (Specify)

Guidance

Effective management and protection of FDA program data and information is needed to ensure the success, and perhaps even the survival, of an FDA program.

FDA data de-identification is a critical aspect of protection and therefore is normally well defined in program standards. The operator will typically provide a clear statement that assures the nondisclosure of flight crew individuals associated with or linked to FDA events, except when it can be determined there is an unacceptable safety risk if specific action regarding the flight crew is not taken.

In general, a successful FDA program requires the establishment of an acceptable level of trust between management and its flight crews. Therefore, the safety intent of the FDA program will be clearly documented so it is understood by all participants, and the conditions of use and protection of program data and information will be explicitly defined in a formal agreement involving the operator's management, representatives of its flight crews and the participating regulatory authority.

More detailed information regarding FDA program data management and protection may be found in the source documents referenced in the guidance associated with ORG 3.3.1.

ORG 3.3.5

△ If the Operator has an FDA program in accordance with ORG 3.3.1, the Operator shall have processes to ensure program findings (e.g. hazards, adverse events and trends, airworthiness issues) are coordinated with relevant operational areas of the organization for further validation and assessment, and for a determination of appropriate follow-up action. Such coordination and follow-up action shall be accomplished within the SMS as follows:

(i) Hazard identification and safety risk assessment and mitigation in accordance with ORG 3.1.1 and ORG 3.2.1.

(ii) Event investigation in accordance with ORG 3.5.1 and ORG 3.5.2.

(iii) Continuing airworthiness assessment in accordance with Maintenance Management Manual (MMM) procedures as specified in MNT 1.7.1 and Table 4.3. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** organizational safety risk assessment/mitigation program (focus: process for analysis of safety data to predict future risks).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected results of data analysis performed to predict future risks.

- ☐ **Examined** examples of action(s) taken to address future risks identified from safety data analysis.
- ☐ **Other Actions** (Specify)

Guidance

Refer to standards in ICAO Annex 6, which specify an FDA program as part of an operator's SMS.

The primary aim of an FDA program is the continuous improvement of the operator's overall safety performance. Therefore, the FDA program, which functions to monitor and measure flight safety performance, is integrated in the Safety Assurance component of the operator's SMS.

The FDA program is also used for safety hazard identification and, as such, is integrated in the Risk Management component of the operator's SMS. Within an SMS there are typically multiple systems used as sources for hazard identification (e.g. accident/incident investigation, operational safety reporting, change management). Therefore, risk management processes are integrated in the operator's SMS to ensure an efficient use of resources and processes, and, where possible, to eliminate or reduce duplicated processes.

Refer to ICAO Doc 9859, Safety Management Manual, and ICAO Doc 10000, Manual on Flight Data Analysis Programmes (FDAP), for more detailed information regarding integration of the FDA program into the operator's SMS.

3.4 Specific Risk Assessments

ORG 3.4.1

The Operator *should* have a policy and procedures for the transport of items in the cargo compartment, which include the conduct of a specific safety risk assessment. Such risk assessment should, as a minimum, include consideration of the following factors:

(i) Hazards associated with the properties of the items to be transported;

(ii) Capabilities of the operator;

(iii) Operational considerations (e.g. area of operations, diversion time);

(iv) Capabilities of the aircraft and its systems (e.g. cargo compartment fire suppression capabilities);

(v) Containment characteristics of unit load devices;

(vi) Packing and packaging;

(vii) Safety of the supply chain for items to be transported;

(viii) Quantity and distribution of dangerous goods items to be transported. **(GM)**

Note: *Mitigation resulting from the safety risk assessment should ensure, to an acceptable level of risk, that in the event of a fire involving items in the cargo compartment, such fire will be detected and sufficiently suppressed or contained by the aircraft cargo compartment fire protection system until a safe landing can be made.*

Note: *Effective 1 September 2024, this recommended practice will be upgraded to a standard; IOSA registration will require conformance by the Operator.*

Auditor Actions

- ☐ **Identified/Assessed** policy and procedures for the transport of items in the cargo compartment: (focus: policy and procedures include safety risk assessment for all items).
- ☐ **Identified/Assessed** process for risk assessment/mitigation (focus: includes involvement of applicable operational disciplines; assessment considers all specified factors; mitigation measures are developed).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** records/documents that illustrate the safety risk assessment process for selected cargo compartment items (focus: all applicable disciplines involved; all specified factors considered; risk mitigation measures developed and integrated in the appropriate operational disciplines).

- ☐ **Coordinated** to verify safety risk mitigation measures for items are implemented in the appropriate operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of COMAT (Company Material).

The intent of this provision is the management of risks associated with the transport of items that, either individually or collectively, might produce a fire that could exceed the cargo compartment fire suppression capabilities demonstrated during aircraft certification (e.g. lithium batteries).

The term 'items' as specified in this provision includes all of the following:

- Cargo (including COMAT and stores);
- Passenger and crew checked baggage;
- Mail;
- Onboard equipment used in the transport of cargo, baggage, or mail (e.g. unit load devices).

The safety risk assessment specified in this provision is not intended to be conducted by the operator on a flight-by-flight basis, but rather conducted initially to establish a baseline risk rating for all types of items that might be transported in the cargo compartment of aircraft during normal operations.

If an operator deviates from the operations that defined the initial risk assessment, then such assessment would be revisited or updated to ensure new hazards have not been introduced by the change in operations. And, even if there are no changes to operations, the risk assessment would be revisited periodically as part of the operator's overall safety management activities to proactively mitigate safety risks before they result in an accident or serious incident.

The type of goods that an operator routinely accepts for transport can directly affect the considerations for hazard identification. For example, an operator that *primarily* transports live animals and perishables (e.g. flowers, fresh food) could reasonably conclude that the risk of a fire, which is a possible consequence of some hazards, is lower than the transport of general cargo. Likewise, the transport of cargo that is itself a potential ignition source would pose a higher risk of fire than the transport of general cargo.

Operators carrying COMAT would have procedures that control the type, quantity, and packaging of such items to be transported. Special procedures, similar to those required for special cargo, would be needed to transport some items of COMAT.

As specified in item (vii), a safety risk assessment would consider the possibility of hazards that might result from or be associated with the supply chain of items that will be transported in the cargo compartment of the operator's aircraft. The process of moving items from origin to destination (i.e. the supply chain) is often very complex. Items might be handled by different entities with varying responsibilities (e.g. shippers, postal operators, freight forwarders, ground handlers, air operators) and could include different modes of transport (e.g. sea, road, rail) as well as different flights. In addition, there could be regional variances in performance that raise the hazard probability. Therefore, to identify the probability of hazards associated with the supply chain process, an operator might consider an analysis of data that can indicate the possibility of any of the following:

- Damage to items through any part of the supply chain;
- Shippers deliberately or unintentionally offering dangerous goods for transport without declaring them;
- Shippers improperly classifying, packing, marking or labelling dangerous goods;
- Freight forwarders accepting undeclared dangerous goods from shippers;
- Dangerous goods prohibited in the mail;
- Passengers carrying prohibited dangerous goods in baggage.

It is the responsibility of the aircraft design approval holders to provide core technical information to operators regarding the technical capabilities of the elements of the aircraft related to fire detection and suppression/extinguishing as required by the applicable certification requirements. The operator can conduct an effective safety risk assessment on the transport of items in a cargo compartment only if there is a full understanding of the performance capability of the cargo compartment systems,

as well as the overall aircraft systems, to handle any identified hazard associated with a particular item.

More detailed information may be found in ICAO Doc 10102, Guidance for Safe Operations Involving Aeroplane Cargo Compartments.

3.5 Occurrence Handling

ORG 3.5.1

The Operator shall have a process for the investigation of aircraft accidents and incidents, to include reporting of events in accordance with requirements of the State. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** accident investigation process (focus: process includes compliance with regulatory accident/incident reporting requirements; output includes final report with recommendations).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected accident and incident reports (focus: investigation identifies operational safety hazards, produces recommendations to prevent recurrence/mitigate risk).
- ☐ **Other Actions** (Specify)

Guidance

Accident and incident investigation is considered a *reactive* hazard identification activity in an SMS.

A primary purpose of accident and incident investigation is hazard identification, which is an element of the Safety Risk Management component of the SMS framework.

Investigations typically result in a report that describes the factors that contributed to the event, which is then made available to responsible senior operational managers to permit them to evaluate and implement appropriate corrective or preventive action.

An effective investigation process typically includes:

- Qualified personnel to conduct investigations (commensurate with operation size);
- Procedures for the conduct of investigations;
- A process for reporting investigative results;
- A system for implementing any corrective or preventive action;
- An interface with relevant external investigative authorities (when applicable);
- A process for the dissemination of information derived from investigations.

To ensure awareness among operational personnel, information derived from investigations is disseminated to relevant areas throughout the organization.

In the event of a major accident, an operator responds to and possibly participates in an investigation in accordance with provisions contained in ICAO Annex 13. Such capability requires an operator to maintain an ongoing interface with relevant investigative authorities to ensure preparedness in the event a major accident occurs.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 3.5.2

The Operator shall have a process for identifying and investigating irregularities and other non-routine operational occurrences that might be precursors to an aircraft accident or incident. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** process for identification/investigation of irregularities/non-routine occurrences (focus: process output includes final report with recommendations).
- ☐ **Interviewed** responsible manager(s).

- ☐ **Examined** selected irregularity/non-routine occurrence reports (focus: process identifies operational safety hazards, produces recommendations to mitigate risk).
- ☐ **Other Actions** (Specify)

Guidance

Investigation of operational irregularities is considered a *reactive* hazard identification activity in an SMS.

A primary purpose of investigating non-routine operational occurrences is hazard identification, which is an element of the Safety Risk Management component of the SMS framework.

The investigation of irregularities or non-routine occurrences is a hazard identification activity. Minor events, irregularities and occurrences occur often during normal operations, many times without noticeable consequences. Identifying and investigating certain irregular operational occurrences can reveal system weaknesses or deficiencies that, if left un-checked, could eventually lead to an accident or serious incident. These types of events are referred to as accident *precursors*.

A process to monitor operations on a regular basis permits the identification and capture of information associated with internal activities and events that could be considered precursors. Such events are then investigated to identify undesirable trends and determine contributory factors.

The monitoring process is typically not limited to occurrences, but also includes a regular review of operational threats and errors that have manifested during normal operations. Monitoring of normal operations can produce data that further serve to identify operational weaknesses and, in turn, assist the organization in developing system solutions.

As with the investigation of accidents and serious incidents, the investigation of minor internal occurrences results in a report that is communicated to relevant operational managers for analysis and the possible development of corrective or preventive action.

Expanded guidance may be found in the ICAO SMM, Document 9859.

3.6 Cybersecurity Risk Management

ORG 3.6.1

The Operator *should* ensure critical information and communications technology systems and data used in operations and maintenance functions are identified and, in accordance with risk management principles, appropriate measures are developed and implemented to protect them from unlawful interference. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** definition of critical information and communications technology systems and data.
- ☐ **Interviewed** manager and/or designated management representative(s).
- ☐ **Examined** selected records/documents that demonstrate application of the process.
- ☐ **Coordinated** to verify implementation of process in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

The protection of critical technology systems and data from unlawful interference will typically include a risk management process to ensure:

- Critical information and communications technology systems and data used in operations and maintenance functions are identified;
- Threats relevant to the identified assets are analyzed to determine corresponding risks to operations and maintenance functions;
- Risks are assessed to determine, develop and implement the required risk mitigation measures or actions.

Examples of communications technology systems and data used in operations and maintenance functions could include the following:

- Flight planning/dispatch systems and data used to support it
- Load control systems and data
- Aircraft performance calculation systems and data
- Reservation/DCS systems
- Baggage reconciliation systems
- EFB (Electronic Flight Bag)
- Aircraft maintenance systems/MCS
- Training and scheduling/rostering systems
- Communication systems/ACARS
- Navigation systems

The process of risk assessment, which is established at the operations life cycle and maintenance level, would include the following steps:

- Define how to identify the risks that could cause the loss of confidentiality, integrity, and/or availability of your critical information and/or data.
- Define how to identify the risk owners for each risk.
- Define criteria for assessing consequences and assessing the likelihood of the occurrence.
- Define how the risk will be calculated.
- Define criteria for accepting risks.
- Risk owners accept the residual risks and approve the risk treatment plan.

The identification and categorization of critical information and communications technology systems and data would be based on an impact analysis. Once this step is completed, each identified asset would go through the evaluation of threats against it, the development of security requirements and the selection of security controls that will protect it.

The selection of security controls, which support technical, operational and management security performance requirements and are within the confidentiality, integrity, and availability (CIA) context, would ideally follow relevant guidance where available.

After implementation of the selected security controls, the operator would continue to assess cyber threats relative to the identified assets, determine any residual risks to aircraft operations and determine the need for additional mitigating actions to supplement or replace existing security controls.

Refer to SEC 4.1.1 for expanded information related to cybersecurity and cybersecurity threats to civil aviation.

4 Improvement and Promotion, Training

4.1 Management Review

ORG 4.1.1

The Operator shall have a process to review the management system at intervals not exceeding one year to ensure its continuing suitability, adequacy and effectiveness in the management and control of operations and associated risks. A review shall include assessing opportunities for improvement and the need for changes to the system, including, but not limited to:

(i) Organizational structure;
(ii) Defined safety objectives;
(iii) Reporting lines, authorities, responsibilities;
(iv) Policies, processes and procedures;

(v) Allocation of resources;
(vi) Identification of training needs**. [SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** corporate management review process (focus: process identifies organizational opportunities for changes/improvement to management system).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Examined** selected records of management review meetings.
- ☐ **Examined** selected examples of output from management review process (focus: changes implemented to improve organizational performance).
- ☐ **Other Actions** (Specify)

Guidance

Management review is a necessary element of a well-managed company that provides a medium through which organizational control and continual improvement can be delivered. To be effective, a formal management review takes place on a regular basis, typically once or more per year. The management review would focus on the entire management system, including the assessment of the effectiveness of the SMS processes.

The management review would typically be conducted by a strategic committee of senior management officials that are familiar with the workings and objectives of the management system. If the review of the SMS is conducted separately, such committee is typically referred to as a Safety Review Board (SRB), which is a very high level, strategic committee chaired by the AE and composed of senior managers, including senior line managers responsible for functional areas in operations (e.g. flight operations, engineering and maintenance, cabin operations).

To ensure frontline input as part of the review process, an operator would form multiple units of specially selected operational personnel (e.g. managers, supervisors, frontline personnel) that function to oversee safety in areas where operations are conducted. Such units are typically referred to as Safety Action Groups (SAGs), which are tactical committees that function to address implementation issues in frontline operations to satisfy the strategic directives of the SRB.

An appropriate method to satisfy this requirement is a periodic formal meeting of senior executives. The agenda of the meeting would typically include a general assessment of the management system to ensure all defined elements are functioning effectively and producing the desired operational safety outcomes consistent with defined safety objectives.

Senior management ensures deficiencies identified during the management review are addressed through the implementation of organizational changes that will result in improvements to the management system.

Input to the management review process would typically include:

- Results of audits;
- Findings from operational inspections and investigations;
- Operational feedback;
- Incidents and near-miss reports;
- Changes in regulatory policy or civil aviation legislation;
- Process performance and organizational conformance;
- Status of corrective and preventative actions;
- Results from implementation or rehearsal of the emergency response plan (ERP);
- Follow-up actions from previous management reviews;
- Feedback and recommendations for management system improvement;
- Regulatory violations.

Output from the management review process would typically include decisions and actions related to:

- Improvement of the processes throughout the management system;
- Safety and security requirements;
- Resource needs.

The management review is a formal process, which means documentation in the form of meeting schedules, agendas and minutes are produced and retained. Additionally, the output of the management review process would normally include action plans for changes to be implemented within the system where deemed appropriate.

Examples of strategies that might improve the overall effectiveness of the management review process include:

- Integrating the management review meeting into other performance review meetings;
- Scheduling management review meetings frequently enough to ensure any action that might be required is timely;
- Ensuring senior managers understand their responsibilities as part of the review process;
- Ensuring action items resulting from meetings are documented and progress is tracked;
- Ensuring there is always a responsible name associated with action items.

Expanded guidance related to review of the SMS may be found in the ICAO SMM, Document 9859.

ORG 4.1.2

The Operator shall have a process to ensure significant issues arising from quality assurance and risk management are subject to management review in accordance with ORG 4.1.1. **[SMS] (GM)** ►

Note: *Conformity with this provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** corporate management review process (focus: quality assurance and risk management issues are included in the management review process).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Interviewed** quality assurance program manager.
- ☐ **Examined** selected records/documents of management review (focus: specific issues/changes identified/implemented to improve quality assurance and risk management programs).
- ☐ **Coordinated** to verify management review of significant quality assurance issues in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Management review supports safety performance monitoring and continuous improvement of the SMS, which are elements of the Safety Assurance component of the SMS Framework.

Such review permits senior management to consider quality assurance and risk management issues that have the potential to affect the safety of operations and then ensure appropriate corrective or preventive actions are implemented and are being monitored for effectiveness in preventing accidents and incidents.

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

☐ **ORG 4.1.3**

The Operator shall have processes to monitor and assess its SMS processes in order to maintain or continually improve the overall effectiveness of the SMS. **[SMS] (GM)**

Auditor Actions

- ☐ **Identified/Assessed** SMS review process (focus: processes for monitoring and assessing SMS to maintain/improve safety performance).
- ☐ **Interviewed** AE and/or designated management representative(s).

- ☐ **Examined** selected examples of output from SMS review process (focus: changes implemented to maintain/improve organizational safety performance).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Safety Assurance, Safety Action Group (SAG) and Safety Review Board (SRB).

Safety performance monitoring and measurement is an element of the Safety Assurance component of the SMS framework.

Monitoring and assessing the effectiveness of SMS processes would normally be the function of a strategic committee of senior management officials that are familiar with the workings and objectives of the SMS. Such committee is typically referred to as a Safety Review Board (SRB), which is a very high-level, strategic committee chaired by the AE and composed of senior managers, including senior line managers responsible for functional areas in operations (e.g. flight operations, engineering and maintenance, cabin operations).

To ensure frontline input as part of the SMS review process, an operator would form multiple units of specially selected operational personnel (e.g. managers, supervisors, frontline personnel) that function to oversee safety in areas where operations are conducted. Such units are typically referred to as Safety Action Groups (SAGs), which are tactical committees that function to address implementation issues in frontline operations to satisfy the strategic directives of the SRB.

Expanded guidance may be found in the ICAO SMM, Document 9859.

4.2 Safety Communication

ORG 4.2.1

The Operator shall have a system that enables effective communication of safety and operational information throughout the management system and in all areas where operations are conducted. Such system shall ensure:

△
(i) Personnel maintain an awareness of the SMS;

(ii) Safety-critical information is conveyed;

(iii) External service providers are provided with information relevant to operations conducted. **[SMS] (GM) ►**

Auditor Actions

- ☐ **Identified/Assessed** organizational communication system (focus: safety and operational information is communicated throughout the organization and to relevant external service providers).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Examined** examples or records of information communication.
- ☐ **Interviewed** selected management system personnel.
- ☐ **Coordinated** to verify implementation of communication system in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Safety communication is an element of the Safety Promotion component of the SMS framework.

An effective communication system ensures the exchange of operational and safety-related information throughout all areas of the organization and includes senior managers, operational managers and front-line personnel.

To be totally effective, the communication system would also include external organizations that conduct outsourced operational functions. Communication with external service providers would typically be limited to information that is pertinent and relevant to the provider's services delivered to the operator. It would be at the operator's discretion to define the extent and content of such communication and the delivery method(s) to be used.

Methods of internal communication will vary according to the size and scope of the organization. However, to be effective, methods are as uncomplicated and easy to use as is possible and facilitate the reporting of operational deficiencies, hazards or concerns by operational personnel.

Specific methods of communication between management and operational personnel could include:

- Email, Internet;
- Safety or operational reporting system;
- Communiqués (e.g. letters, memos, bulletins);
- Publications (e.g. newsletters, magazines).

If email is used as an official medium for communication with operational personnel, the process is typically formalized by the operator to ensure control and effectiveness.

The general intent of safety communication is to foster a positive safety culture in which all employees receive ongoing information on safety issues, safety metrics, specific hazards existing in the workplace and initiatives to address known safety issues. Such communication typically conveys safety-critical information, explains why particular actions are taken to improve safety and why safety procedures are introduced or changed.

Information and issues relevant to safety performance are typically derived from various sources such as, but not limited to, the quality assurance/flight safety analysis programs, operational safety reporting and accident/incident investigations.

Expanded guidance may be found in the ICAO SMM, Document 9859.

4.3 Training

ORG 4.3.1

The Operator shall have a program that ensures its personnel are trained to understand SMS responsibilities and competent to perform associated duties. The scope of such training shall be appropriate to each individual's involvement in the SMS. **[SMS] (GM) ►**

Note: *The specifications of this provision are applicable to personnel of the Operator.*

Note: *Conformity with this ORG provision is possible only when the Operator is in conformity with all repeats of this provision in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** SMS training program (focus: program ensures training for the operator's personnel as appropriate to individual SMS involvement).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected SMS training curricula/syllabi (focus: personnel are trained to understand SMS responsibilities and to perform associated SMS duties).
- ☐ **Examined** selected management/non-management personnel training records (focus: completion of SMS training relevant to individual involvement in the SMS).
- ☐ **Coordinated** to verify SMS training is implemented in all operational areas.
- ☐ **Other Actions** (Specify)

Guidance

SMS training is an element of the Safety Promotion component of the SMS framework.

Within an operator's organization there are personnel that perform duties that are directly or indirectly related to the safety of aircraft operations. All such personnel thus have an involvement in the operator's SMS. This applies to management and non-management personnel in frontline operational positions and could also include others that perform certain administrative functions. The intent of this provision is for the operator to have a program that ensures personnel are trained and competent to perform their SMS duties. Such program would include training for support staff, operational personnel, managers and supervisors, senior managers and the accountable executive.

The content of safety training is appropriate to each individual's involvement in the SMS and typically includes or addresses some or all of the following subject areas:

- Organizational safety policies, goals and objectives;
- Organizational safety roles and responsibilities related to safety;
- Organizational SMS processes and procedures;
- Basic safety risk management principles;
- Safety reporting systems;
- Human factors.

Recurrent training would be offered at the option of the operator to ensure personnel maintain continuing competency in SMS duties. If offered, such training would typically focus on changes to SMS policies, processes and procedures as well as any specific safety issues relevant to the organization.

An operator may use various methods to verify if personnel are competent to perform their duties at the conclusion of the training. The methods used would be solely at the discretion of the operator and would typically be based on the depth and detail of the training provided. Such methods may include a combination of the following:

- Including knowledge checks during the training modules;
- Performing Q&A sessions at the conclusion of a module or training session;
- Including practical exercises with feedback;
- Observing the staff member during the performance of SMS duties;
- Administering an oral or written test;

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

Expanded guidance may be found in the ICAO SMM, Document 9859.

ORG 4.3.2

If the Operator outsources operational functions to external service providers, the Operator *should* have a program that ensures personnel of external service providers are trained to understand SMS responsibilities and perform associated duties. The scope of such training *should* be appropriate to individual involvement in the Operator's SMS. **[SMS] (GM)** ►

Note: *The specifications of this provision are applicable to personnel of an external service provider that performs operational functions for the Operator.*

Note: *Conformity with this ORG recommended practice is possible only when the Operator is in conformity with all repeats of this recommended practice in other ISM sections.*

Auditor Actions

- ☐ **Identified/Assessed** SMS training program (focus: program ensures training for personnel of external service providers as appropriate to individual SMS involvement).
- ☐ **Interviewed** SMS manager and/or designated management representative(s).
- ☐ **Examined** selected outsourcing contracts/agreements (focus: inclusion of requirement of SMS training for service provider personnel).
- ☐ **Examined** selected records/reports resulting from monitoring of service providers (focus: monitoring process ensures personnel of service providers have completed SMS training).
- ☐ **Coordinated** to verify SMS training for external service provider personnel is implemented in applicable operational areas.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Operational Function.

SMS training is an element of the Safety Promotion component of the SMS framework.

If an operator outsources operational functions, it would typically define initial and recurrent training standards to ensure training of service provider personnel is consistent with and meets the requirements of its own SMS.

Recurrent training for personnel of providers, although recommended, would be specified at the option of the operator.

Training in accordance with this provision may be conducted by the operator, or by the service provider or other organization as long as the content and delivery of such training satisfies the SMS requirements of the operator.

The scope and content of such training would typically take into account the following:

- Training required for personnel that would perform the same operational function within the operator's organization;
- Individual personnel function(s) as related to the operator's SMS;
- Exposure and/or involvement of the provider's personnel to the operational environment;
- SMS elements the service provider already has in place.

Based on a risk assessment and considering the above factors, an operator may conclude that SMS training is not required for personnel of providers that perform certain operational functions.

An operator might consider any of the following options as means for ensuring personnel of service providers complete training that satisfies the requirements of its own SMS:

- If a service provider has an SMS, accept the service provider's SMS training;
- If a service provider has an SMS, specify training in addition to that of the service provider (i.e. gap training) as applicable to ensure its own SMS requirements are satisfied;
- Have applicable personnel of service providers complete the operator's own SMS training;
- Deliver targeted or specific SMS training to personnel of service providers (e.g. hazard recognition, use of the operational safety reporting system).

Refer to the IAH for information that identifies repeats of this ORG provision in other ISM sections.

4.4 Effectiveness

ORG 4.4.1

The Operator *should* demonstrate that systems, processes and procedures specified in the ISARPs identified with the **[Eff]** symbol are achieving the designated Desired Outcome.

Note: *Conformity with this ORG provision is possible only when the Operator demonstrates effectiveness of implementation for all ISARPs designated with the **[Eff]** symbol.*

Note: *Conformity with this provision does not require specifications to be documented by the Operator.*

Auditor Actions

☐ **Coordinated** to verify status of conformity with ISARPs designated with the **[Eff]** symbol.

☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Desired Outcome and Effective.