Section 8 — Security Management (SEC)

Applicability

Section 8 addresses the management of operational security in accordance with requirements of an Air Operator Security Program (AOSP). This section is applicable to all operators.

Individual SEC provisions or sub-specifications within a SEC 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.

Where operational security functions are outsourced to contracted external service providers, an operator retains responsibility for the conduct of such functions and will have processes to monitor applicable external service providers in accordance with SEC 1.11.2 to ensure requirements that affect the security of operations are being fulfilled.

General Guidance

Definitions of technical terms used in this ISM Section 8, 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

SEC 1.1.1

The Operator shall have a security management system (SeMS) that includes, as a minimum, the following key elements:

(i) Senior management and corporate commitment;
(ii) Resource management;
(iii) Threat assessment and risk management;
(iv) Management of emergencies and incidents (resilience);
(v) Quality control and quality assurance;
(vi) Air Operator Security Program (AOSP). **(GM)**

Auditor Actions

☐ **Identified/Assessed** supervision and control functions of the AOSP.
☐ **Examined** relevant sets of security standards.
☐ **Interviewed** responsible manager(s).
☐ **Other Actions** (specify).

Guidance

Refer to the IRM for the definitions of Air Operator Security Program (AOSP), Operator and Security Management System (SeMS).

Conformity with the provisions in Subsection 1, Management and Control, would typically demonstrate evidence that an operator has implemented an SeMS that meets the requirements of this standard.

Conformity with this standard may be achieved by incorporating the following elements into the SeMS:

- Senior management and corporate commitment:
  - Appointment of a Head of Security;

    - Security department organizational structure;
    - Authorities and responsibilities;
    - Delegation of duties.
- Resource management:
    - Staff selection process;
    - Staff performance assessment process;
    - A security personnel training program;
    - Security awareness training program;
    - Management of service providers.
- Threat assessment and risk management:
    - Identification of risks and threats;
    - Threat assessment;
    - Risk management.
- Management of emergencies and incidents (resilience):
    - Emergency preparedness and response;
    - Crisis and contingency management plans;
    - Security incident management.
- Quality control and assurance:
    - Reporting and corrective actions mechanisms;
    - Oversight of external service providers.
- Air Operator Security Program (AOSP).

Provided all the above elements are implemented, individual operators may group or break down the elements and sub-elements in a manner that best suits their own structure.

An operator's SeMS is structured to ensure the most efficient and effective application of the AOSP.

The SeMS is typically documented in the form of a manual or other appropriate controlled medium, and includes detailed descriptions of the structure, individual responsibilities, available resources and processes in place to effectively manage security operations and ensure an operator is in compliance with the requirements of the civil aviation security program of the State.

An operator typically documents security procedures in a manual or, as applicable, more than one manual (e.g. where operational security responsibilities are delegated to various departments or by geographic locations, each with distinct security requirements). All documents comprising an operator's operational security manual (or equivalent document) are considered controlled documents.

Where permissible, the AOSP, rather than being documented separately in a security manual or equivalent, may be incorporated into the same manual (or other controlled medium) and thus be documented as an integral part of the SeMS.

An operator may differentiate between policy and procedure manuals. A policy manual typically states goals and objectives while a procedural manual outlines detailed action-oriented steps that, when complied with, will meet the policy.

Additional guidance may be found in the IATA Security Management System Manual (http://www.iata.org/publications/store/Pages/security-management-system-manual.aspx).

Refer to Guidance associated with ORG 1.1.1 located in ISM Section 1.

SEC 1.1.2

The Operator shall have a senior management official designated as the head of security with direct access to the highest level of management within the organization. Such senior management official, regardless of other functions and reporting structure, shall:

(i) Be responsible for ensuring implementation and maintenance of the AOSP;

(ii) Have overall accountability for ensuring operations are conducted in accordance with conditions and restrictions of the AOSP and in compliance with applicable regulations and standards of the Operator. **(GM)**

Auditor Actions

- ☐ **Identified** individual designated as the head of security.
- ☐ **Examined** corporate organizational structure.
- ☐ **Examined** job description of the head of security (focus: functions include implementation/maintenance of the AOSP).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (specify).

Guidance

Refer to the IRM for the definitions of Accountability and Responsibility.

Based on the size, structure and complexity of an operator's organization, the position of head of security could be filled by a member of senior management that has responsibilities in addition to security. However, the organization is structured, it is important that one senior management official is the designated focal point for security management on behalf of the operator.

SEC 1.1.3

The Operator shall have a corporate security policy that states the commitment of the organization to a culture that has security as a fundamental operational priority. Such policy shall be communicated throughout the organization and commit the organization to:

(i) The provision of resources necessary for the successful implementation of the policy;
(ii) Compliance with applicable regulations and standards of the Operator;
(iii) The promotion of security awareness and the establishment of a security culture;
(iv) The establishment of security objectives and security performance standards;
(v) Continual improvement of the SeMS;
(vi) Periodic review of the policy to ensure continuing relevance to the organization. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** corporate security policy (focus: policy identifies security as fundamental operational priority).
- ☐ **Examined** examples of security policy communication (focus: communication methods, organizational awareness campaign).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Just Culture.

The security policy of an organization typically expresses the clear and genuine commitment by senior management to the establishment of a security culture. Such policy also defines the organization's fundamental approach toward security and how security is expected to be viewed by employees and external service providers.

When an operator has an integrated management system (e.g. SMS, QMS) that includes SeMS, the security policy may be incorporated in the corporate safety and/or compliance monitoring policy. The security policy might include the following elements to ensure the comprehensive integration of security:

- The adoption of industry best practices for security management where warranted;
- Continual management review and improvement of the SeMS and security culture;
- The development of objectives for the measurement of security performance;

- Imperatives for including operational security in the description of duties and responsibilities of senior and frontline management;
- The promotion of a reporting system that encourages the reporting of inadvertent human error and/or intentional acts of non-compliance;
- Communication processes that ensure a free flow of information throughout the organization.

In addition to a formal security policy document, an operator would typically have documented dissemination channels that can contribute to awareness of the policy and its content among all employees and establish security as a priority for everyone.

States and the Industry have developed different promotional tools for security incident awareness and reporting. The use of IATA's "See it Report it" training and certification tool is one method for an operator to demonstrate conformity with this provision. (https://www.iata.org/whatwedo/security/Pages/security-management-system-sems.aspx)

The organizational security policy typically expresses the operator's focus on achieving an effective security culture that protects the safety and security interests of its employees, customers, shareholders, assets and brand. Such policy also ensures that obligations contained in domestic and international aviation security laws and regulations are met.

The security policy usually specifies minimum security requirements and identifies applicable reference documents (e.g. the AOSP). It also defines the roles and responsibilities of management and non-management employees, and those with specific security accountabilities.

The security policy typically addresses the yearly establishment of KPIs for the head of security and but for the entire organization. Review of the KPIs provides the basis for the following year's program objectives including the allocation of resources to achieve such objectives. This review typically includes the impact of the security culture, identification of non-compliances including associated corrective actions, reported incidents along and root cause analysis. Trends identified are then used to define new security objectives.

Finally, the security policy will normally state the operator's commitment to proactively managing risk, complying with legislation and regulations, aligning security activity with assessed risk and implementing a 'just culture' to encourage security-related reporting.

1.2 Air Operator Security Program (AOSP)

SEC 1.2.1

The Operator shall have a formal Air Operator Security Program (AOSP) that includes:

△
(i) The requirements of the civil aviation security program of the State of the Operator (hereinafter, the State);

(ii) Supplementary Station Procedures (SSP) that meet the requirements of other states where operations are conducted;

(iii) The security standards of the Operator. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** the AOSP.
- ☐ **Examined** operator-specific security requirements and standards.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Acts of Unlawful Interference, State, State Acceptance and State Approval.

An operator is required to have a AOSP in order to:

- Protect customers, personnel, assets and customer goods from any act of unlawful interference;
- Comply with regulatory requirements.

The name of an operator's security program may vary based on the regulatory jurisdiction. Examples of typical alternative names to AOSP include ACSP (Air Carrier Security Program) and ASP (Airline Security Program).

☐ With regard to Supplementary Station Procedures (SSP), as this is a new concept recently introduced in ICAO Annex 17 (Amendment 18) some states may still require air operators to develop country-specific AOSPs in order to operate into third country. In such a scenario, the operator will typically have an AOSP approved by its state of registry and a number of AOSPs approved by third country regulators.

△ The Security Program may be structured in accordance with the template provided by the State.

The State may issue a standard security program with which all operators must comply (operators may apply for exemptions or amendments, as applicable). In such cases, the standard security program of the State is typically recognized as the AOSP of the operator. The AOSP typically also includes or refers to other company manuals and procedures that provide operator-specific details.

△ A standard security program may be acceptable in meeting security requirements of other states, or the operator may be required to submit supplementary station procedures tailored to meet requirements of other states. An operator must satisfy the security requirements of all applicable states for the purpose of meeting the intent of this provision. Typically, a state of operation will consider an AOSP letter of approval by the Operator's state of registry along with the required supplementary station procedures as an acceptable security program to operate within its borders.

The AOSP may be approved or accepted (i.e. no notice of deficiency or equivalent is issued) by the relevant state.

The AOSP may include security sensitive information as required by the State. In such case, the AOSP would normally include a description of dissemination of security sensitive information in a way that ensures the required level of data protection.

Refer to Guidance associated with SEC 1.4.1 for additional information.

1.3 Authorities and Responsibilities

SEC 1.3.1

The Operator shall ensure the SeMS defines the authorities and responsibilities of management personnel within the SeMS and provides a general description of security responsibilities for categories of non-management personnel within the SeMS as documented in the AOSP. The SeMS shall specify:

(i) The levels of management with the authority to make decisions that affect operational security;

(ii) Responsibilities for ensuring security functions are performed and procedures are implemented in accordance with applicable regulations and standards of the Operator;

(iii) Lines of accountability throughout the SeMS, including direct accountability for security on the part of senior management;

(iv) Responsibilities of members of management, irrespective of other functions, as well as of non-management personnel, with respect to security performance of the SeMS. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** defined management/non-management authorities and responsibilities throughout the SeMS.
- ☐ **Interviewed** designated management representative(s).
- ☐ **Examined** job descriptions of selected management/non-management personnel in security management.
- ☐ **Other Actions** (Specify)

Guidance

Refer to Guidance associated with ORG 1.3.1 located in ISM Section 1.

SEC 1.3.2

The Operator shall have a process or procedure for delegation of duties and assignment of responsibilities within the SeMS that ensures managerial continuity is maintained when managers with operational security responsibilities are unable to carry out work duties. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** processes for delegation of duties when managers with operational security responsibilities are absent (focus: processes maintain managerial continuity during periods when managers are absent).
- ☐ **Interviewed** designated security management representative(s).
- ☐ **Examined** selected example(s) of delegation of duties due to absence.
- ☐ **Other Actions** (Specify)

Guidance

Such plan addresses responsibilities associated with management positions (not individuals) under the AOSP and ensures proper management of operational security functions is always in place.

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.

To achieve conformity with this provision, an operator would be expected to demonstrate how a delegate is chosen, how and when (i.e. under what circumstances) a delegation is activated and how this is communicated to those with a need to know. Such process can be activated manually when required or automatically under specific conditions.

Procedures are also typically established to delegate the authority to address and take act in response to new and emerging risks, threats as well as incidents taking place at any moment during the operation. Delegation of such responsibilities will typically be given to a group of employees either designated to be on call or to be part of the operator's 24/7 operations center.

Refer to Guidance associated with ORG 1.3.2 located in ISM Section 1.

SEC 1.3.3

The Operator shall ensure a delegation of duties and assignment of responsibility for liaison with applicable aviation security authorities and other relevant external entities. **(GM)**

Auditor Actions

- ☐ **Identified** position(s) with authority for liaison with regulators and other external entities.
- ☐ **Interviewed** designated management representative(s).
- ☐ **Interviewed** manager(s) with authority for liaison with regulators and other external entities.
- ☐ **Examined** job description for selected management positions (focus: authority/responsibility for liaison with external entities).
- ☐ **Other Actions** (Specify)

Guidance

Although motives might be different, all stakeholders share a similar interest in ensuring the security of the aviation industry. However, the potential problem of gaps or overlap in responsibilities and/or coverage may exist when more than one entity is handling security. It is crucial for state, airport and airline security officials to establish clear jurisdictional boundaries to ensure all entities understand where their respective jurisdictions begin and end.

Whereas gaps in security create obvious problems and expose the entire aviation infrastructure to threats, the presence of unnecessary overlap by different security groups can also lead to problems. Without proper coordination, the presence of multiple entities providing security services could lead to inaccurate assumptions that might, in fact, result in unintended gaps in the security web due to a reduction of services. Also, multiple groups doing the same job could lead to conflicts of authority, which would detract from the required focus on aviation security.

It is important that there is effective communication between airport security and airline security management. An Airline Operators Committee typically offers a viable platform for airlines and an airport authority to express their respective views on security and identify areas of deficiency. Such committee might also serve as a useful forum for coordination between airlines and airports to develop and implement a seamless security system with no gaps and appropriate overlap.

With regards to state involvement, the creation of an Airport Security Committee (ASC) might be suggested since the group would focus solely on security and address only security issues.

It is recommended that operators participate in both the Airline Operators Committee and the ASC, either directly or via representation by other carriers or stakeholders.

1.4 Communication

SEC 1.4.1

The Operator shall have a system that enables effective communication of security information throughout the management system and all areas where operations are conducted. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** system(s) for communicating information relevant to security operations (focus: capability for communicating information relevant to operations within the security organization).
- ☐ **Interviewed** designated management representative(s).
- ☐ **Examined** examples of information communication in security operations.
- ☐ **Interviewed** selected non-management operational personnel in security operations.
- ☐ **Other Actions** (Specify)

Guidance

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

Security information that is sensitive is typically drafted and circulated in a manner that is in accordance with applicable security information protocols. Communication of such information is normally limited only to those with an operational need to know.

Any system would have to be able to address the varying degree of urgency with which security information needs to be circulated.

Security Intranet Site

A corporate security department website is one method of disseminating security information to operational personnel. Different levels of access might be required in order to control the access to restricted information to those with a “need to know.” Corporate security awareness information and security incident reporting forms or templates are typically made available on this website. However, where various management systems (e.g. QMS, SMS, SeMS) are aligned or integrated, there may be one common form or template accessed from a central location that is used for reporting incidents.

Corporate Manual System

An operator's manuals and regulations are the formal system of coordinating and communicating the policies, procedures and significant guidance necessary to ensure the operator's mission is carried out in a consistent and integrated manner.

Security Bulletins

Security bulletins, which are typically issued by the corporate security department or by operational departments within the operator, might specify action and/or contain general information. Issuance of bulletins electronically (e.g. email) is an efficient means of ensuring all personnel with a "need to know" are made aware of new or amended security information in a timely manner.

Refer to Guidance associated with ORG 4.2.1 located in ISM Section 1.

1.5 Provision of Resources

SEC 1.5.1 (Intentionally open)

△ **SEC 1.5.2**

The Operator shall have a selection process for management and non-management positions within the scope of AOSP, to include positions within the organization of the Operator and if applicable, service providers selected by the Operator that conduct operational security functions. 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 and methods for selection of personnel in functions relevant to safety and security of aircraft operations.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Interviewed** selected personnel that perform security functions relevant to the safety or security of aircraft operations.
- ☐ **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 safety and security operations.

Refer to Guidance associated with ORG 1.5.3 located in ISM Section 1.

SEC 1.5.3

If permitted by the State, the Operator shall ensure a process has been established that requires operational security personnel in the organization of the Operator and, if applicable, service providers selected by the Operator to conduct operational security functions, to be subjected to pre-employment and recurring background checks in accordance with requirements of applicable aviation security authorities. The requirement for a background check shall be applicable to personnel who:

(i) Engage in the implementation of security controls;
(ii) Have unescorted access to the security restricted area of an airport;
(iii) Have unescorted access to other security areas and searched aircraft;
(iv) Have access to sensitive aviation security information. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process for the pre-employment and recurring background checks.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records of personnel background checks.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Security Control and Security Restricted Area.

A background check might include:

- Criminal record check;
- Previous employment history;
- Personal references;
- Education and training.

National legislation on civil liberties and protection of personal information will greatly influence the limits placed on an employer when performing pre-employment background checks. An employer is not permitted to deviate from the laws of the country where the hiring process is taking place.

Escorted access may be provided to an individual that has yet to complete all aspects of the background checking process.

An individual currently permitted unescorted access to a security restricted area, but who subsequently fails to satisfy the criteria to continue to hold an airport identification card or for unescorted access to a security restricted area, will typically have access to security restricted areas, as well as access to sensitive aviation security information, revoked immediately.

The operator's role in the background check process will be determined by the State. In some cases, the entire process will be managed and/or conducted by the State.

1.6 Documentation System

△ **SEC 1.6.1–1.6.2** (Intentionally open)

△ **SEC 1.6.3**

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, and in the implementation of the AOSP and its associated SSPs to ensure that they:

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

(ii) Contain legible and accurate information;

(iii) 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 AOSP and its associated SSPs.

☐ **Interviewed** responsible management representative(s).

☐ **Examined** selected parts of the security manual (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. Refer to ORG 2.5.1 and associated Guidance, and Table 1.1, located in ISM Section 1.

States may impose new protection measures on sensitive aviation security information.

The operator will typically have a central source of information for security procedures that is automatically updated in case of approved changes. Old versions would be archived for historical purposes.

△ The current version or authorized version of AOSP and its associated SSPs documentation would typically be in an electronic form and found in a specific/dedicated library. Printed versions are usually deemed to be uncontrolled copies. Employees would have to know how to gain copies from the single information source and that a new copy must be produced to ensure use of a current document version.

△ **SEC 1.6.4**

If the Operator has external service providers conduct outsourced operational security functions, the Operator shall have a process to ensure such external service providers receive information regarding security directives and instructions in a timely and secure manner that meets requirements of the AOSP and its associated SSPs. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to circulate relevant security information to external service providers.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected examples of information provided to external service providers.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Outsourcing.

The operator would have a central source of information for security procedures that is automatically updated in case of approved changes. Obsolete versions would only be accessible for archiving/historical purposes. The main source of information would be electronic and found in a specific/dedicated library. Printouts of the procedures would be considered as backup solutions. Personnel of a service provider with a need to know would have to know how to obtain or access copies from the single information source and that a new copy must be produced to ensure use of a current document version.

1.7 (Intentionally open)

1.8 Records System

SEC 1.8.1

The Operator shall have a system for the management and control of operational security records to ensure the content and retention of such records is in accordance with requirements of the aviation security authority of the State, as applicable, and to ensure security 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, including retention and storage as mandated by the State. **(GM)** ◄

Auditor Actions

- ☐ **Identified/Assessed** management and control system for operational records in security operations (focus: system includes standardized processes as specified in standard).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Examined** selected records required to be kept by the aviation security authority of the State.
- ☐ **Other Actions** (Specify)

Guidance

Some security records could contain sensitive or restricted information that, while not classified, could be detrimental to aviation security if publicly released. Such restricted information is typically defined, usually in conjunction with specific handling procedures, by the State or the operator.

Typical handling procedures for records containing sensitive or restricted information ensure:

- When not in the physical possession of an authorized person, paper or physical records are stored in a secure container such as a locked file cabinet or drawer. Electronic records are stored in a file folder that has restricted access and/or encryption;
- A review is conducted periodically (typically once per year) to identify records that are no longer valid and to ensure such records are destroyed in a manner that precludes recognition or reconstruction of the information.

States may impose additional protection measures on sensitive aviation security information that could be contained in security records.

The operator will typically have a central source of information for security procedures that is automatically updated in case of approved changes. Obsolete versions of electronic records would be accessible for archiving/historical purposes.

The current or authorized version of records would typically be filed electronically in a specific dedicated library. Printed versions of records are usually deemed to be uncontrolled copies.

Access to security records will typically be limited to individuals with a need to know. These individuals would have been provided guidance on how to properly access security records ensuring that the most recent and up to date version is accessed.

Refer to Guidance associated with ORG 2.6.1 located in ISM Section 1.

SEC 1.8.2

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** management and control system for operational records in security operations (focus: system defines schedule for periodic file backup).
- ☐ **Interviewed** responsible management representative(s).
- ☐ **Examined** selected record(s) of backup files for electronic records.
- ☐ **Other** Action (Specify)

Guidance

Refer to Guidance associated with ORG 2.6.2 located in ISM Section 1.

1.9 Management Review

△ **SEC 1.9.1**

The Operator shall have a security review committee for the purpose of ensuring:

(i) Senior management oversight of security in operations;
(ii) Continual improvement of the SeMS;
(iii) Security threats are being identified and controlled;
(iv) The promotion of security awareness. **(GM)**

Auditor Actions

- ☐ **Identified/Examined** the security review committee functionality and/or terms of reference.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected review committee reports/meeting notes.
- ☐ **Examined** selected examples of meeting outcome implementation.
- ☐ **Other Actions** (Specify)

Guidance

A security review committee, which might have a different name with each operator, would ideally be chaired by the Accountable Executive or designated security official, and usually includes the head of security, other members of senior management and representatives from the major operational areas.

A security review committee typically meets at least every two months to review the security performance in operations, address security concerns, provide feedback and instructions to the operating units, and set priorities for sub-teams. It may be useful to have more frequent meetings in the first year of establishment to create an awareness of the committee throughout the organization.

SEC 1.9.2

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

Auditor Actions

- ☐ **Identified/Assessed** SeMS review process (focus: processes for monitoring and assessing SeMS to maintain/improve security performance).
- ☐ **Interviewed** AE and/or designated management representative(s).
- ☐ **Examined** selected examples of output from SeMS review process (focus: changes implemented to maintain/improve organizational security performance).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Safety Management System (SMS) and Security Management System (SeMS).

Monitoring and assessing the effectiveness of SeMS processes would typically be the function of a strategic committee of senior management officials that are familiar with the workings and objectives of the SeMS.

Depending on the operator's organizational structure, the effectiveness of SeMS may be monitored and assessed by the same executive group that is responsible for the SMS or the security review committee.

Refer to guidance associated with ORG 4.1.1 located in ISM Section 1. Such guidance addresses continual improvement of an SMS but could be adapted and applied for continual improvement of SeMS. Additional guidance is also available in section 2.4 of the IATA SeMS Manual.

1.10 Quality Assurance/Quality Control Programs

Quality Assurance

SEC 1.10.1

The Operator shall have a quality assurance program that provides for the auditing and evaluation of the management system and operational security functions at a determined frequency following a regularly performed risk assessment to ensure the organization is:

△

(i) Complying with the AOSP and its associated SSPs and other applicable regulations and standards;

(ii) Satisfying stated operational needs;

(iii) Identifying areas requiring improvement;

(iv) Identifying threats to operations;

(v) Assessing the effectiveness of security risk management and controls. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** role/organization/structure of quality assurance program (focus: role/purpose within organization/SeMS; definition of audit program scope/objectives; description of program elements/procedures for ongoing auditing of management/operational areas).
- ☐ **Interviewed** responsible quality assurance program manager.
- ☐ **Interviewed** selected operational managers (focus: interface with quality assurance program).
- ☐ **Examined** selected security organization audit reports (focus: audit scope/process/ organizational interface).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Quality Assurance (QA) and Security Risk.

△ The quality assurance program will typically determine compliance with the AOSP and its associated SSPs.

△ Typically, the person responsible for the security operation is accountable for the implementation of a quality assurance program, which includes the various standards set out within the AOSP and its associated SSPs. The quality assurance program typically takes into consideration the standards set by other states to achieve specific requirements as the result of their respective risk analyses and threat assessments.

Quality Assurance refers to all areas of security protection and prevention that involve the operator, handling agents, personnel, passengers and the carriage of cargo and aircraft stores. It also incorporates an examination of the actions or inactions of airports and other agencies, which, although not directly “touching” the airline, could impact on the security of the operator.

△ To achieve the set objectives of the AOSP and its associated SSPs, it is necessary to introduce a means of measuring the efficiency and effectiveness of the security operation and to note any deficiencies.

Operators typically perform a security risk assessment at least once a year. The frequency of security audits is then typically determined on a risk-priority basis as determined by the operator for its operations at its base and overseas stations. There are two main purposes for conducting a security audit:

△
- To ensure operator personnel, handling agents and contractors are properly implementing the AOSP and its associated SSPs;

△
- To ensure the AOSP and its associated SSPs are achieving the set objectives.

Personnel involved in the performance of audits are normally trained and have the necessary qualifications required by the State.

Audits may be complemented by quality control mechanisms, to include:

- Security Inspections to confirm the level of regulatory compliance;
- When authorized by the State, security tests to evaluate the effectiveness of specific aviation security measures and procedures;
- Security exercises to evaluate the effectiveness of the emergency response plan.

Refer to Guidance associated with ORG 2.1.1 located in ISM Section 1.

SEC 1.10.2

The Operator shall have a process for addressing findings resulting from audits of operational security functions that 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 security area(s);

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

Auditor Actions

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

Guidance

Executive managers of organizational business units are responsible for making sure quality assurance activity is undertaken to ensure:

- Conformity with the security standards;
- Existence of required security systems;
- Compliance with relevant aviation security legislation;
- Conformity with IOSA and the SeMS standards.

Auditors conducting quality assurance activities apply the internal audit procedure. This manual, IOSA ISARPS, and the internal assessment tool form the basis for quality assurance activity.

Information and data taken from audit reports or an equivalent business tool are used to record all quality assurance activity. Individual business units are responsible for identifying and assigning corrective actions to the appropriate personnel for implementation, completion and follow-up monitoring for effectiveness.

Corrective actions are managed in accordance with internal quality assurance processes and procedures.

For each audit finding a root cause is identified and corrective action developed as appropriate to address the root cause. Corrective action is then implemented in the appropriate operational security areas and evaluated to determine effectiveness in addressing the root cause.

To ensure findings are corrected in a timely manner, it is important for the operator to have a process that clearly identifies the owner of the deficient process and delegates responsibility to that owner to develop and implement the appropriate corrective action(s).

It is also important to establish a clear timeline to implement the appropriate corrective action(s) as well as have a process to escalate to senior management when deadlines are missed.

Refer to Guidance associated with ORG 2.1.7 located in ISM Section 1.

SEC 1.10.3A

The Operator shall have a process to ensure significant issues arising from quality assurance audits of operational security functions are subject to a regular review by senior security management. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process to inform senior security management of significant issues identified through quality assurance audits (focus: continual improvement of quality assurance program).
- ☐ **Interviewed** responsible quality assurance program manager.
- ☐ **Examined** selected records/documents of management review of security organization quality assurance program issues (focus: specific issues/changes identified and implemented to improve quality assurance program).
- ☐ **Other Actions** (Specify)

Guidance

In order to ensure proper implementation of corrective actions following the identification of gaps or deficiencies through quality assurance audits, it is important that senior security management is made aware of overall audit reports and especially of any significant issue(s) identified.

Senior security management officials have the authority and available expertise to quickly resolve any deficiency in order to prevent re-occurrences and ensure that the corrective actions implemented are commensurate to the gaps or issues identified.

Auditor recommendations contained in a report provide the basis for possible changes within the system. However, for various reasons, the adoption or implementation of recommendations made by auditors may not always be feasible. Therefore, the determination of a need for corrective or preventive action, and the actual implementation of such action, would typically be coordinated between the Head of Security (or appointee) and those operational managers directly responsible for the safety and security of operations.

Refer to Guidance associated with ORG 4.1.2 located in ISM Section 1.

SEC 1.10.3B

The Operator shall have an audit planning process and sufficient resources, including auditors as specified in ORG 2.1.8, to ensure audits are:

(i) Scheduled in accordance with a security risk assessment at intervals to meet regulatory and management system requirements;

(ii) Conducted within the scheduled interval (subject to a change in risk). **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** planning process for quality assurance auditing of security functions.
- ☐ **Identified/Assessed** resources (human and physical) allocated and available for auditing.
- ☐ **Interviewed** responsible quality assurance program manager.
- ☐ **Crosschecked** audit plan with selected audit reports (focus: conduct of audits by planned dates).
- ☐ **Other** Action (Specify)

Guidance

△ The frequency of auditing activity is typically determined by ongoing risk assessments to ensure business units are complying with the applicable AOSP and its associated SSPs, achieving the applicable AOSP and its associated SSPs objectives and properly applying security standards.

A desktop risk assessment using risk-based evaluation tools aligned with internal standards is usually undertaken to determine the associated frequency for audits. An annual audit plan based on the assessment results is then produced.

These audit plans are then provided to the management for consolidation of all audit requirements into a financial year audit plan. Audit plans identify frequency, auditee, audit function and location. Management will identify and confirm sufficient resources to acquit the plan and submit the consolidated audit plan back to the business units for approval.

To achieve conformity with this provision, tracking/monitoring progress against the audit plan will be demonstrated by the operator.

Refer to Guidance associated with ORG 2.1.5 located in ISM Section 1.

Quality Control

SEC 1.10.4 (Intentionally open)

SEC 1.10.5

If required and/or authorized by the aviation security authority, the Operator shall have a process for conducting security tests that assess the effectiveness and proper implementation of security controls of which the Operator is in direct control. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process for conducting security tests required and/or authorized by the aviation security authority.
- ☐ **Interviewed** responsible manager(s).

- ☐ **Examined** selected security test result reports, other evidence of evaluation of effectiveness.
- ☐ **Other Actions** (Specify)

Guidance

A security test is a simulated act of unlawful interference against existing security measures, carried out covertly by persons using an approved test object concealed in their baggage or on their person. Similar tests are also sometimes performed on cargo shipments and in aircraft. Tests may be used for ensuring alertness of security personnel, which might be considered with caution because the results of testing could degrade the motivation of such personnel.

An effective testing program ensures the administration of tests:

- Are only conducted where permitted by the laws of the state(s) where such tests are conducted;
- Do not jeopardize the safety of persons;
- Do not jeopardize the safety of aircraft or airport facilities;
- Do not damage property;
- Do not alarm or inconvenience the public and persons or organizations not being tested;
- If required, includes notification of applicable police authorities and other security agencies.

Furthermore, tests may be conducted:

- In accordance with a schedule;
- Without prior notification to the operating or supervisory personnel (management, however, is made aware);
- Using clearly marked test pieces (decoys);
- By qualified personnel who are in possession of documentation authorizing such testing.

SEC 1.10.6

If required and/or authorized by the aviation security authority, the Operator shall have a process to perform or participate in periodic operational security exercises in order to:

(i) Evaluate the effectiveness of procedures designed for response to security incidents;

(ii) Practice implementation of security procedures by applicable personnel. **(GM)**

Auditor Actions

- ☐ **Identified** the process for conducting security exercises required and/or authorized by the aviation security authority.
- ☐ **Examined/Assessed** security exercise process, including scheduling and evaluation mechanism.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected reports of previous security exercises.
- ☐ **Other Actions** (Specify)

Guidance

If the Operator is invited to participate in an emergency response exercise (where a security element may be addressed), or wishes to conduct its own emergency response exercise, the Operator will be able to correct any deficiencies discovered as a result of plan implementation.

If the opportunity to participate in a full-scale emergency exercise is not possible, an operator may conduct a table-top security exercise.

1.11 Quality Control of Outsourced Operations and Products

SEC 1.11.1A

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

(i) Security-relevant selection criteria are established;

(ii) Service providers are evaluated against these criteria prior to selection. **(GM)** ◄

Auditor Actions

- ☐ **Identified/Assessed** selection process for external service providers.
- ☐ **Interviewed** responsible manager(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 aviation security 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.

Refer to the guidance associated with ORG 1.6.1.

SEC 1.11.1B

If the Operator has external service providers conduct outsourced operational security functions, the Operator shall have a process to ensure a contract or agreement is executed with such external service providers. Such contract or agreement shall identify the application of specific documented requirements that can be monitored by the Operator to ensure requirements that affect the security of its operations are being fulfilled by the service provider. **(GM)** ◄

Auditor Actions

- ☐ **Identified/Assessed** process to execute contracts or agreements with external security service providers.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected contracts/agreements used for external security service providers.
- ☐ **Other Actions** (Specify)

Guidance

The contract or agreement typically includes the measures required and associated performance measures (perhaps in a supplemental service level agreement) to be met by the service provider.

△ To satisfy the monitoring specification of this provision, service providers (or contractors) that provide security services required under the AOSP and its associated SSPs would typically receive planned inspections and/or audits by the operator.

Normally, an operator obtains a written undertaking that ensures service providers are familiar and comply with standards of the operator and local regulatory requirements.

An important aspect to be monitored by the operator would be the security training provided to personnel of the service provider(s).

The use of the Standard Ground Handling Agreement contained in the IATA Airport Handling Manual typically signifies that the provider is in conformity with this provision.

The use of a registered ISAGO provider typically signifies that the provider is in conformity with basic industry security requirements.

Refer to Guidance associated with ORG 1.6.2 located in ISM Section 1.

SEC 1.11.2

If the Operator has external service providers conducting outsourced operational security functions, the Operator shall have processes to monitor such external service providers to ensure requirements that affect the 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 used for monitoring external service providers (focus: monitoring process ensures provider fulfils applicable safety/security requirements).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records/reports of monitoring of external service providers.
- ☐ **Other Actions** (Specify)

Guidance

The contract and/or agreement may contain those aspects of the Security Program and/or regulatory requirements to be undertaken by the external service provider. In most cases only one or two aspects of the AOSP may be involved, which would negate the requirement to provide or monitor compliance with the entire AOSP.

Examples of activities that might be used to verify such compliance include:

- Periodic quality assurance audits of providers conducted by the operator using either corporate or local resources;
- Reports submitted to the operator by the provider detailing self-audit schedules and results;
- Quality control functions (e.g. security surveys/tests) conducted jointly by the operator and provider.

The use of a registered ISAGO provider typically signifies that the provider is in conformity with basic industry security requirements.

Refer to Guidance associated with ORG 2.2.1 located in ISM Section 1.

SEC 1.11.3 (Intentionally open)

SEC 1.11.4

If the Operator has operational security functions conducted by external organizations not under the control of the Operator, the Operator shall have methods, as permitted by the applicable civil aviation security authority, for the monitoring of such functions to ensure, as permitted, implementation of outsourced security measures is in compliance with its AOSP. **(GM)**

Auditor Actions

- ☐ **Identified** operational security functions conducted by external organizations not under the control of the operator.
- ☐ **Identified/Assessed** methods used by the operator for monitoring functions to ensure that security controls are implemented.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records of monitoring the external organizations that conduct security functions.
- ☐ **Other Actions** (Specify)

Guidance

Security procedures may be performed by law enforcement agencies, civil aviation authorities, airport authorities or other organizations not under the control of or under contract to the operator. When the operator has no direct authority over the organization performing the security measures, oversight and verification functions could be performed via inspections and reporting in case of incidents or deviation from the standard operating procedures.

If permitted by law or the applicable civil aviation security authority, the operator might assess the quality of such security procedures through the use of tests, surveys and/or exercises.

This standard is applicable to all security procedures required under the security program of the State, state of operation or the operator.

1.12 Operational Reporting

SEC 1.12.1

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

(i) Encourages and facilitates personnel to report security incidents and security occurrences pertaining to the Operator;

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

(iii) Includes analysis and management action as necessary to address security issues identified through the reporting system. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** system for operational personnel to report security incidents and security occurrences (focus: system urges/facilitates reporting of security/safety concerns; includes analysis/action to validate/address reported security/safety concerns).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected reports submitted by operational personnel.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Just Culture, Security Incident, Security Occurrence, Security Vulnerability and Security Threat.

Frontline personnel, such as flight or cabin crew members, maintenance technicians and ground handling personnel, are in the best position to note abnormalities that could indicate real or potential security threats, or any other security concerns, so they may be brought to the attention of the head of security and other relevant managers.

Applicable aviation security authorities would be notified in accordance with SEC 4.3.2 when a legitimate security incident or security occurrence has been identified through the operational security reporting system.

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

A system that encourages and promotes reporting from personnel might include:

- A process that protects the confidentiality of the report;
- A process that provides for review by corporate security personnel;
- An articulated Just Culture policy that encourages reporting of security incidents or events, even if resulting from human error;
- A shared responsibility between personnel (or, if applicable, respective professional associations) and management to promote the confidentiality of the reporting system;
- A process for secure de-identification of reports;
- A tracking process of action taken in response to reports;
- A process to provide feedback to the reporter, when appropriate;
- A communication process for ensuring frontline operational personnel, as well as other relevant personnel, are apprised of potential security issues through dissemination of de-identified report information.

An operational reporting system is implemented as permitted by law or as restricted by other specified obligations placed on an operator.

A security reporting system, regardless if developed separately or in conjunction with other operational reporting system(s), is normally designed in a way that enables analysis and the undertaking of necessary actions.

Typically, an operator's reporting system includes its own staff and, as applicable, that of service providers as reporting is a service provider's obligation under the IATA Standard Ground Handling Agreement provisions.

Qualitative and quantitative analysis of security data would be facilitated if the operator uses a harmonized taxonomy for the classification of reports. In this regard, an operator might refer to the IATA Safety Incidents Taxonomy (ISIT), which includes security taxonomy. Expanding harmonized taxonomy to service providers would benefit security threat, vulnerability and event analysis by allowing for more consistency, benchmarking and security performance measurement.

IATA has established a new database system called the Incident Data Exchange (IDX). IDX will permit operators to report security incidents and security occurrences for uploading into the IDX safety management database for subsequent analysis by users. The IDX submission process requires submission of security incident and security occurrence reports using a common taxonomy (ISIT) that is aligned with the IDX security taxonomy. See SEC 4.3.3, which addresses the reporting of security incidents and security occurrences to IATA for inclusion in the IDX.

Refer to ORG 3.1.2 and ORG 3.1.3 located in ISM Section 1 for information that addresses an operational safety reporting systems.

SEC 1.12.2

The Operator shall have a process to ensure security information, security incidents, security occurrences and acts of unlawful interference that have been reported by personnel in accordance with SEC 1.12.1 or are derived from states or other relevant sources are reviewed by operational and security management to ensure:

(i) Root cause is identified;

(ii) A security risk assessment is conducted;

(iii) Corrective action is determined;

(iv) When applicable, corrective action is implemented and monitored to ensure effectiveness in preventing future incidents or occurrences. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** security risk management process (focus: incidents, occurrences, acts of unlawful interference derived from internal reporting and external sources is evaluated and, as applicable, subjected to the security risk management process).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected security risk management reports (focus: root causes identified, risks assessed, corrective actions developed and implemented/monitored).
- ☐ **Other Actions** (Specify)

Guidance

An effective process provides for a review and analysis of each report to determine the risk associated with the reported issue and, where applicable, ensures development and implementation of appropriate action by responsible management to correct the situation.

In addition, an effective process provides for a review and analysis of information derived from each report and from external sources to determine the need for risk assessment and, when applicable, the development and implementation of appropriate risk control action by responsible management to mitigate the security risk. Effective security risk management ensures security information, security incidents and acts of unlawful interference are acted upon under a security methodology that evaluates and address security threats, vulnerabilities and associated consequences.

2 Training and Qualification

2.1 Training Program

△ **SEC 2.1.1**

The Operator shall have a security training program that is approved or accepted by the State and meets applicable requirements of other states. Such program shall consist of initial, recurrent and, where applicable, requalification training that comprises, as appropriate, theoretical training, practical training and an assessment of competencies to ensure:

(i) Personnel, employed by or under the control of the Operator who implement security controls understand security awareness and reporting, and have the competence to perform their duties;

(ii) Flight and cabin crew members, as well as frontline aircraft ground handling and cargo handling personnel, are able to act in the most appropriate manner to minimize the consequences of acts of unlawful interference and disruptive passenger behavior. **(GM)**

Note: *If permitted by the State, the program shall ensure applicable personnel have completed appropriate security background checks in accordance with SEC 1.5.3 prior to attending any training that contains sensitive or restricted security information.*

Note: *Applicable personnel shall complete initial security training prior to being assigned to operational duties.*

Auditor Actions

- ☐ **Identified/Assessed** security training program (focus: approval/acceptance by State; meets applicable requirements of other states; background checks required prior to personnel attending training).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected security training program curricula (focus: contain theoretical and practical training elements).
- ☐ **Examined** selected ground/cargo handling personnel training records (focus: completion of initial/recurrent security training).
- ☐ **Other Actions** (Specify)

Guidance

Training may be sub-divided for line managers/supervisors, aircrew, ramp workers, cargo personnel and other personnel who are directly involved in the implementation of security measures and thereby require an awareness of obligations to the AOSP.

The security training program is typically integrated into the normal training curriculum for operational personnel and need not be stand-alone training.

The proportion of theoretical and practical training is typically based on requirements of the State. For certain functions or duties there may not be a practical component.

The scope of recurrent security training, as well as the specific subject matter included, may vary in accordance with requirements of the applicable authorities and the security policy of the operator.

☐ The assessment of competencies to ensure the objectives of the training have been met is typically done via testing, on the job assessment or a combination of both. The passing mark and required elements in the assessment of competencies are usually determined by the State.

An existing background check from a previous employer may be acceptable if still time valid.

Different training tools for security awareness and security incident reporting have been developed by states and the Industry. The use of IATA's "See it Report it" training and certification tool is one method for the operator to demonstrate conformity with the relevant specification in this provision. (https://www.iata.org/whatwedo/security/Pages/security-management-system-sems.aspx)

SEC 2.1.2

If the Operator has operational security functions conducted by external service providers selected by the Operator (outsourcing), the Operator shall have a process to ensure such external service providers have a security training program that:

(i) Is acceptable to the Operator;

(ii) Consists of initial, recurrent and, where applicable, requalification training;

(iii) Includes, as appropriate, theoretical and practical training;

☐ (iv) Includes an assessment of competencies;

(v) Ensures personnel have a common understanding of security awareness and reporting. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to ensure external service providers have security training programs.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected evidence that ensures external service provider(s) have a security training program that meets the specifications in this provision.
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for an operator to ensure its security requirements are being satisfied by service providers at all stations at which it operates. In states where providers are prohibited from divulging security information, it might be necessary for the operator to seek access from the local regulatory authority or attempt access through diplomatic channels. In some cases, the host country regulator may be requested to obtain the applicable security information as part of its station audits, which typically ensure security training for providers at the station meets local and/or ICAO requirements.

When a service provider will not provide access to its security training program, the operator can seek to reach an agreement whereby the service provider uses the operator's training program. If such agreement is not possible, then, depending on other options available and the type(s) of services to be provided, the operator could conduct a risk assessment to determine the need to select another provider.

☐ The assessment of competencies to ensure that the objectives of the training have been met is typically done via testing, on the job assessment or a combination of both. The passing mark and required elements in the assessment of competencies are usually determined by the State. If such standards are not established by the State, the external service provider will typically be required by the operator to have passing thresholds similar to the Operator,

SEC 2.1.3 (Intentionally open)

SEC 2.1.4

The Operator shall ensure personnel who perform security functions, crew members and appropriate operational personnel, as specified in SEC 2.1.1, complete recurrent security training on a frequency in accordance with requirements of the security program of the State and, if applicable, other states where operations are conducted or, if there is no regulatory mandate, not less than once every 36 months. **(GM)**

Auditor Actions

- ☐ **Identified** requirements mandating frequency of recurrent training (focus: compliance with requirements of the State and other relevant states; if there is no regulatory mandate, not less than once every 36 months).
- ☐ **Examined** selected recurrent training records, material and schedules.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

The scope of recurrent security training, as well as the specific subject matter included, may vary in accordance with requirements of the applicable authorities and the security policy of the operator.

SEC 2.1.5

If the Operator manages a security screening system, the Operator shall ensure personnel who manage or operate the screening system:

(i) Are approved and/or certified in accordance with requirements of the applicable aviation security authority;

(ii) Complete initial and recurrent training that includes training in the identification of explosives, weapons or other dangerous items or devices. **(GM)**

Auditor Actions

- ☐ **Identified** security screening system(s) managed or operated by operator.
- ☐ **Identified/Assessed** screener approval/certification program (focus: in compliance with requirements of all applicable aviation securities authorities).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected initial/recurrent screener training curricula (focus: training includes identification of explosives/, weapons/other dangerous items/devices).
- ☐ **Examined** selected initial/recurrent screener training records (focus: completion of training in identification of explosives/, weapons/other dangerous items/devices).
- ☐ **Other Actions** (Specify)

Guidance

When a screener certification program exists, an operator is normally required to ensure all screeners are certified by the applicable aviation security authority. In locations where there is no screener certification program, the operator typically provides a level of training to all screeners that ensures such personnel are able to properly detect and identify all explosives, components of improvised explosive devices, weapons and other dangerous items or devices.

Continuing competency is normally maintained through recurrent training on a frequency that is in accordance with requirements of the applicable aviation security authority.

The approval/certification of personnel who manage or operate the screening system would typically include:

- A check of the person's reliability (initial and recurrent background check).
- Completion of initial and recurrent training specific for the job function, to include:
  - Theoretical, practical and on-the-job training.
  - Training on the use of screening equipment to enhance capabilities for detecting explosive materials and/or explosive devices, whether carried by persons or within any item screened.
- Evidence of formal approval/certification accomplished either by or on behalf of the relevant aviation security authority.

Screeners undertaking cargo screening duties are typically not looking for weapons. Such personnel are normally trained to detect and identify improvised explosive devices, including individual components, and unauthorized dangerous goods.

SEC 2.1.6

The security training program of the Operator shall include a process for reviewing and updating or revising security training courses to ensure:

(i) Continual improvement of curriculum, including content and applicability to the operational environment;

(ii) Incorporation of regulatory amendments or operational changes. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) for review/updating security training courses (focus: emphasis on continual improvement/applicability to operational environment).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected security training curricula revisions (focus: incorporation of regulatory amendments/operational changes).
- ☐ **Other Actions** (Specify)

Guidance

A training review/revision program will typically consist of:

- A risk-based training needs analysis by the operator's security department;
- A check against the current regulatory framework;
- A check against current & emerging security threats;
- Reaction/experience of the trainee with respect to training relevance/added value by means of questionnaire;
- An assessment of training effectiveness through measurement of operational performance or observation of trainee performance;
- Consideration of cost effectiveness.

SEC 2.1.7

The Operator shall ensure the completion of required security training by operational personnel is documented and retained in a records system in accordance with SEC 1.8.1.

Auditor Actions

- ☐ **Identified/Assessed** security training record keeping process(es) (focus: security training for all operational personnel documented/recorded).
- ☐ **Interviewed** responsible management manager(s).
- ☐ **Examined** selected security training records (focus: retention in accordance with SEC 1.8.1).
- ☐ **Other Actions** (Specify)

SEC 2.1.8

The Operator shall ensure operational personnel complete security awareness training that focuses on preventative measures and techniques in relation to passengers, baggage, cargo, mail, equipment, stores and supplies, as applicable, and permits such personnel to contribute to the prevention and reporting of acts of sabotage, other forms of unlawful interference and security occurrences. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** requirement to complete security awareness training for operational personnel.
- ☐ **Examined** security awareness training program contents and selected training records.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Security awareness training revolves around ensuring all personnel have a positive attitude about security. The focus of training to achieve such awareness will vary by region or company and may be influenced by cultural, religious and other factors. Such training is typically tailored to promote an organizational security culture and to be effective in the environment in which it is to apply. Some operators, depending on the individual organizational structure, may find it more appropriate to have multiple security awareness training courses developed specifically for each operating area. Security awareness training may be integrated into other job-related training courses (as opposed to a standalone course).

Typically, operational personnel that complete security awareness training are crew members, frontline ground handling personnel and all personnel that implement security controls irrespective of whether such personnel are directly employed by the operator or employed by external service providers.

☐ Typically, security awareness training programs will include an assessment of competencies. The assessment of competencies to ensure that the objectives of the training have been met is typically done via testing, The passing mark and required elements in the assessment of competencies are usually determined by the State.

Different training tools for security awareness and security incident reporting have been developed by states and the Industry. The use of IATA's "See it Report it" training and certification tool is one method for the operator to demonstrate conformity with the reporting specification in this provision. (https://www.iata.org/whatwedo/security/Pages/security-management-system-sems.aspx).

3 Security Operations

3.1 Access Control

SEC 3.1.1

If the Operator has exclusive control over airport airside areas and/or security restricted areas, the Operator shall ensure an identification verification system is in place that prevents personnel and vehicles from unauthorized access. Such identification system shall include:

(i) Designated checkpoints where identification is verified before access is permitted;

(ii) A requirement for authorized personnel to prominently display an identification badge. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** identification verification system in place to prevent unauthorized access to airport security restricted area(s).
- ☐ **Identified** designated checkpoints where identification is verified.
- ☐ **Identified** system used to ensure all authorized personnel prominently display their identification badge.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Access to airside and security restricted areas is often the responsibility of the airport operator or a designated government agency. At those airports where an operator has exclusive control over a specific area within the airside or the security restricted area, it is the responsibility of the operator to control access through its managed checkpoints.

In most cases the identification badge is issued by the airport authority or a designated government agency. It is not expected that an operator will need to develop its own identification system, provided the airport operator or government agency system is sufficient.

SEC 3.1.2

The Operator shall ensure measures are in place to control and supervise personnel and vehicles moving to and from the aircraft in security restricted areas to prevent unauthorized access to the aircraft. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** measure(s) to control and supervise the movement of personnel and vehicle to and from the aircraft in the security restricted area(s)
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Procedures are in place to ensure airline personnel intercept any person identified as having no need to be on board or near the aircraft.

In some environments, it would be prudent not to leave an in-service aircraft unattended. Precautions may be taken to prevent unauthorized access to aircraft that are not in service and are parked and unattended. For example, all external doors may be locked, all stairs and loading bridges are removed (or locked) and any steps left near the aircraft are immobilized.

Passengers boarding or disembarking from flights using the apron are to be supervised when passing from the terminal building to the aircraft. Such measures are applied whether the passengers are walking or are being transported in vehicles.

Particular care is taken to ensure only crew members, authorized representatives and officials, and bona fide passengers are permitted access to the aircraft.

SEC 3.1.3

The Operator shall ensure access control measures and security screening measures as mandated by the State are in place to prevent the introduction of unauthorized weapons, explosives or other dangerous devices or items on board an aircraft by persons other than passengers. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to prevent the introduction of unauthorized weapons, explosives or other dangerous devices on board an aircraft.
- ☐ **Examined** records of the capture and prevention of unauthorized weapons, explosives or other dangerous devices on board an aircraft.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Supernumerary.

Typically, access control and security screening measures will apply to personnel of the operator and service providers, including supernumeraries that are authorized to travel on an aircraft to perform specific duties. Measures that apply to access control and screening of personnel are documented in the AOSP and/or other operational manual(s). The baseline for such measures typically would be that a person:

- Holds a valid authorization to enter a security-restricted area (based on, as a minimum, a background check, operational needs and completion of security awareness training);
- Is subjected to screening (combination of equipment and procedures aimed at identifying and/or detecting all potentially dangerous items, substances, and devices that could be used to commit an attack).

As a reference, ICAO Annex 17 requires states to establish measures to ensure applicable personnel are screened prior to entry airport security restricted area, including use of appropriate screening methods capable of detecting explosives either continuously or in an unpredictable manner.

An effective method to deter or detect illegal access to aircraft is the implementation of frequent but irregularly timed patrols by security personnel. This is particularly important when operations are at their lowest levels and aprons and hangar areas are least frequented. Such patrols are normally conducted by airport personnel.

Additional measures to prevent unauthorized access to passenger aircraft may include:

- Parking aircraft in a well-lit area; adding security lighting, if necessary;
- When possible, parking aircraft in an area visually observable and/or covered by CCTV;
- Parking aircraft away from fences or buildings that might provide easier access;
- For aircraft parked overnight, depending on the assessed risk at the location, applying a tamper-evident seal to all exterior doors accessible without aids or verifying the identity of all persons who access the aircraft to ensure a legitimate reason for accessing the aircraft;

- For aircraft parked remotely from a loading bridge:
  - Closing all exterior doors and exterior hatches of the aircraft;
  - Removing all stairs;
  - Ensuring no portable stairs, lift devices or passenger transfer vehicles are in the immediate vicinity of the aircraft.
- For aircraft parked with access to a loading bridge:
  - Closing all exterior hatches of the aircraft;
  - Closing all exterior doors of the aircraft not served by a bridge;
  - Locking the door between the terminal and the bridge;
  - Ensuring no portable stairs, lift devices or passenger transfer vehicles are in the immediate vicinity of the aircraft;
  - Locking or keeping under constant surveillance doors that provide access to the bridge from the apron or retracting the bridgehead from the aircraft and deactivating the bridgehead positioning controls.

3.2 (Intentionally open)

3.3 Carriage of Weapons

SEC 3.3.1

If the carriage of weapons on board an aircraft by law enforcement officers and/or other authorized persons acting in the performance of their duties is approved by the Operator, the State and/or other applicable authorities, the Operator shall have a policy and procedures, in accordance with the laws of the state(s) involved, for such carriage of weapons. **(GM)**

Note: *Notification to the PIC of authorized armed persons on board occurs in accordance with FLT 3.9.4 and GRH 3.7.5. The content of such notification may vary in accordance with the laws of the state(s) involved in the approval for weapons carriage.*

Auditor Actions

- ☐ **Identified/Assessed** policy and procedures for the carriage of weapons in the cabin of the aircraft.
- ☐ **Examined** selected documents that reflect validity of carrying weapons on board an aircraft.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

The term ‘weapon’ in the context of this provision is normally a firearm legally in the possession of a law enforcement officer or other authorized individual (e.g. an inflight security officer acting in the performance of his or her duties as an armed officer).

An agreed procedure with the relevant law enforcement agency is typically in place that permits the operator to notify the PIC (and other crew members as required by local requirements) of the presence of armed persons on board.

△ Operators will have differing methods to accomplish the booking, seating and notification to the flight crew of armed individuals on board. A clear communication protocol by the operator ensures a consistent booking-to-boarding process for such individuals. The content of such notification may vary in accordance with the laws of the state(s) involved in the approval for weapons carriage.

In accordance with ICAO standards, states that could be relevant to an individual flight (i.e. states of departure, transit, arrival, potential diversion) will have laws that require special authorization for the carriage of weapons on board an aircraft.

Each Contracting State ensures that the carriage of weapons on board aircraft by law enforcement officers and other authorized persons acting in the performance of their duties requires special authorization in accordance with the laws of the States involved.

SEC 3.3.2 (Intentionally open)

SEC 3.3.3

If the carriage of weapons in hold baggage on board an aircraft for a passenger flight is approved by the Operator, the Operator shall have procedures for the carriage of such weapons to ensure:

(i) If the weapon is a firearm or capable of discharging a projectile, the passenger or an authorized and duly qualified person has declared the weapon to be not loaded;

(ii) The weapon is stowed in a place that is inaccessible to any unauthorized person during flight;

(iii) The carriage of a weapon is legally permitted by all state(s) involved, including the State and state(s) of flight departure, transit and arrival. **(GM)**

Auditor Actions

- ☐ **Examined/Assessed** procedures used for the authorization, control and stowage of weapons carried on board.
- ☐ **Identified** persons who are authorized and qualified to determine weapons are not loaded.
- ☐ **Examined** locations where weapons are stowed in the aircraft to confirm they remain inaccessible to unauthorized persons during flight.
- ☐ **Identified/Assessed** procedures to determine that the transport of a weapon is legally permitted in all states involved.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

With the approval of the operator, the following procedures are typically implemented for any weapon carried as hold baggage:

- Prior to acceptance, the passenger or other authorized and duly qualified person determines that the weapon is not loaded. A declaration may be used to confirm the status of the weapon;
- The weapon is transported in a sturdy container to prevent any possible damage during the flight;
- Ammunition is securely boxed and carried separately from the weapon, and is handled in accordance with applicable dangerous goods regulations;
- Weapons and ammunition are stowed in an area that inhibits access by any unauthorized person while the aircraft is in flight; such weapons are not to be carried on the flight deck or retained by any crew member;
- If available, a lockable tamper-proof container located in the aircraft hold is used for this purpose;
- Transit and transfer stations are advised and ensure the integrity of such items;
- At the final destination, when required by the State of Flight Arrival, security procedures are implemented to return the weapons and/or ammunition to the passenger;
- Where the weapon is stowed in a baggage compartment (or hold) that is accessible to persons during flight:
    - The compartment door(s) remain closed and are monitored during the flight;
    - The weapon is packed separately from any ammunition;
    - The weapon is stowed in the compartment in a manner that access is obstructed (or impeded) by other baggage.

3.4 Passengers (Including Supernumeraries) and Cabin Baggage

SEC 3.4.1

If the Operator conducts passenger flights, the Operator shall have a process to ensure originating passengers and their cabin baggage are subjected to screening prior to boarding a passenger aircraft for;

(i) An international flight;

(ii) As required by the applicable aviation security authority, a domestic flight. **(GM)**

Note: *Supernumeraries that require a flight reservation or passenger name record for transport on the aircraft shall be subjected to the requirements of this provision unless exempted by the State.*

Auditor Actions

- ☐ **Identified/Assessed** process(es) to ensure all passengers (including supernumeraries, if applicable) and their cabin baggage are screened prior to boarding a passenger aircraft for international flights.
- ☐ **Identified/Assessed** process(es) for the screening of originating passengers (including supernumeraries, if applicable) and their cabin baggage for domestic flights (if required by the applicable aviation security authority).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** passenger/baggage handling operations (focus: originating passengers/cabin baggage are subjected to screening prior to aircraft boarding).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Domestic Flight.

△ The effective screening of all passengers and their cabin baggage is recognized as an essential element in achieving a safe and secure operation, and forms part of the passenger handling procedures contained in the AOSP and its associated SSPs.

Technical equipment used for the screening of persons and baggage has certain limitations. Archway metal detectors and hand-held metal detectors, for example, cannot detect non-metallic weapons and explosives. Even conventional X-ray equipment does not always image or define explosive material effectively. To compensate for such limitations, or to introduce a random element into the selection process, it may be advisable to conduct an additional search of passengers and cabin baggage after they have been screened. The additional screening can be performed by hand or by technical means, such as explosive trace detection (ETD), full-body X-ray, explosive particle or vapor detection portals and/or other approved advanced technological methods.

It is recommended that screening equipment used to assist screening personnel is capable of detecting explosive materials and/or explosive devices that might be carried by passengers either on their person or in cabin baggage.

If the use of explosive detection screening equipment is not continuous, then it is recommended that such equipment be used on a random basis to ensure non-predictability by passengers and others.

Specific guidelines and procedures are developed and training is given to personnel for addressing persons with special needs.

SEC 3.4.2 (Intentionally open)

SEC 3.4.3

If the Operator conducts passenger flights, the Operator shall have a process to ensure transfer and transit passengers and their cabin baggage *either*:

(i) Are subjected to screening prior to boarding a passenger aircraft, *or*

(ii) Have been screened to an appropriate level at the point of origin and subsequently protected from unauthorized interference from the point of screening at the originating airport to the departing aircraft at the transfer or transit airport. **(GM)**

Auditor Actions

- ☐ **Identified** process(es), when required, to ensure all passengers and their cabin baggage are screened prior to boarding a passenger aircraft.
- ☐ **Identified/Assessed** criteria used to determine whether passengers and cabin baggage are re-screened at the transit/transfer airport or if one-stop-security is applied.
- ☐ **Observed** screening measures being implemented for transfer and transit passenger and their cabin baggage, as applicable.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Unauthorized Interference.

Transit and transfer passengers and their cabin baggage may not require screening prior to admission to an airport sterile area if, in the judgment of the appropriate authority for security, the standard of screening en route and at the airport of embarkation is equal or comparable to that of the admitting state. However, measures ought to be established to ensure transit or transfer passengers do not take unauthorized articles on board an aircraft.

SEC 3.4.4

If the Operator conducts passenger flights, the Operator shall have a process to ensure passengers and their cabin baggage are subjected to additional security controls in accordance with requirements of the applicable aviation security authority when flights are under an increased security threat. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) for ensuring additional security controls for flights under increased security threat.
- ☐ **Observed** additional passenger and cabin baggage security measures implemented based on the various levels of increased security threats.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

In the case of a general (i.e. non-specific) *intermediate* threat level, in addition to the baseline passenger and carry-on screening procedures, the following additional measures may be implemented:

- Continuous random searching of passengers by hand (or by approved technological methods) either at the departure gate (where airport facilities permit) or other suitable location(s).
- Continuous random searching of cabin baggage by hand (or by approved technological means) either at the departure gate (where airport facilities permit) or other suitable location(s).

In the case of a general (i.e. non-specific) *high* threat level, additional measures such as the following may be introduced:

- All departing passengers are searched again by hand or screened with metal detection equipment at the departure gate before being permitted to board the aircraft;
- All cabin baggage is subjected to an additional search by hand or by X-ray equipment, either at the departure gate (where airport facilities permit) or other suitable location(s), before being permitted to be carried on board the aircraft.

If a threat is specific to a certain object (e.g. liquid explosives), then more specific countermeasures than above would need to be implemented.

To facilitate additional screening, earlier close-out of passenger check-in operations is a consideration.

SEC 3.4.5

If the Operator conducts passenger flights, the Operator shall have a process to ensure passengers and their cabin baggage, which have already been subjected to screening, are:

(i) Protected from unauthorized interference from the point of screening until they board a passenger aircraft;

(ii) Subjected to re-screening if the potential for unauthorized interference has been determined to exist. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to determine if passenger re-screening is required.
- ☐ **Identified/Assessed** methods used to ensure passengers are protected from unauthorized interference until they board the aircraft.
- ☐ **Identified/Assessed** process(es) used to determine if unauthorized interference may have been possible.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** passenger/baggage handling operations (focus: process for protecting passengers/cabin baggage from unauthorized interference after screening until aircraft boarding).
- ☐ **Other Actions** (Specify)

Guidance

For domestic flights and for flights between countries that have an equivalent application of security standards and such equivalency is recognized by the relevant state authority, the separation of screened and unscreened passengers and their carry-on baggage is sufficient.

For international flights, if the design of the airport permits, to ensure separation from departing passengers who have been subjected to screening, arriving passengers disembark from an aircraft in accordance with any of the following:

- On a level different from the departure boarding area, or
- Through an area isolated from the departure boarding area; or
- Into an area of the airport dedicated to arriving passengers only.

If physical means to avoid contact between departing and arriving passengers is not possible, passenger mix may be prevented by restricting access to the departure lounge until all arriving passengers have cleared the area. This solution may not be possible in large airport terminals with many gates close to each other.

The major concern regarding the sterility of arriving passengers will most likely be associated with flights that have originated in states where screening requirements are considered to be inadequate by the State of Flight Arrival. In order to limit the disruption of passenger flow within a terminal, consideration might be given to assigning the disembarkation of all such flights to a common sector or area of the airport or terminal that can be cordoned off and/or monitored by security personnel. Where passengers are arriving from a state where screening is considered by the State of Flight Arrival to be equal or better, arriving and departing passengers can mix.

In order to limit the disruption of passenger flow within a terminal, consideration might be given to assigning the disembarkation of all such flights to a common sector or area of the airport or terminal that can be cordoned off and/or monitored by security personnel.

SEC 3.4.6

The Operator *should* ensure security practices and/or procedures for operational security personnel that have contact with passengers include behavior detection methods designed to identify persons who may pose a threat to civil aviation and require additional security measures. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** practices/procedures for behavior detection (focus: recognition of characteristics that indicate anomalous behavior, criteria for resolution and application of additional security measures).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** implementation of appropriate behavior detection practices/procedures.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Behavior Detection.

An operator will typically only include behavior detection methods when it has the responsibility for implementing certain security screening and risk assessment measures to identify passengers that might pose a security threat.

The use of behavior detection methods will typically only be used for regular public transport and open charter passenger flights. Behavior detection is not normally used for government and/or closed charter passenger flights.

In accordance with SEC1.11.4 when behavior detection functions are a government responsibility, an operator will typically have methods, as permitted by the applicable civil aviation security authority, for the monitoring of such functions to ensure, as permitted, implementation is in compliance with its AOSP.

In the framework of a risk-based approach to aviation security, behavioral detection is used to identify persons who may pose a threat to civil aviation and should be subjected to additional security measures. This technique involves the recognition of behavioral characteristics, including but not limited to, physiological or gestural signs indicative of anomalous behavior.

Behavioral detection programs are based on the premise that people attempting to evade security measures typically display signs of anomalous behavior, as compared to the behaviors of the legitimate travelling population. Such programs pinpoint individuals on the sole basis of their behavior and never according to their nationality, ethnicity, race, gender or religion.

A review of existing behavioral detection programs shows that choosing persons for additional security controls on the basis of anomalous behavior can be more effective than selecting persons randomly.

Behavior detection programs in various jurisdictions might vary in terms of methodology and processes. However, typically, such programs employ a four-stage process as follows:

- An environmental baseline is established at a given time and location, within which the anomalous behavior of persons would be identified.
- Persons are observed at pre-determined locations to identify those exhibiting anomalous behaviors which are above the environmental baseline established.
- Anomalous behaviors are resolved through targeted conversation with persons and/or through additional screening.
- If anomalous behaviors cannot be resolved, persons are referred to enhanced security measure or appropriate authorities.

SEC 3.4.7

The Operator shall have a policy and procedures to refuse transportation to any person that does not consent to a search of his or her person or property in accordance with the AOSP. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** the policy and procedures used to deny boarding of a passenger or supernumerary that refuses to consent to security searching or other security control.
- ☐ **Examined** selected documents used when right to deny boarding is communicated to passengers.

- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Persons who refuse to undergo screening before boarding or entering an aircraft are denied boarding and not allowed to pass the point of search. Additionally, such persons, or others who might be denied passage for other security reasons, are referred to policing authority officials, if required by law.

3.5 Special Category Passengers

SEC 3.5.1

If the Operator conducts passenger flights, the Operator shall have a policy and a process that incorporates risk assessment measures to ensure procedures are in place for the transport of potentially disruptive passengers who are obliged to travel because they have been the subject of judicial or administrative proceedings. Such procedures shall be designed to take into consideration the assurance of the safety of the aircraft during the flight. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** policy and process(es) in place for the transport of potentially disruptive passengers.
- ☐ **Identified/Assessed** process(es) used to assess the risk posed by any potentially disruptive passenger.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definitions of Deportee and Inadmissible Passenger.

Airlines that have transported people who have been refused entry to a state can be called upon to return such person(s) to the port of embarkation. Such removal is accompanied by a judicial order of removal.

Those responsible within the organization of an operator for compliance with judicial orders (e.g., station managers) inform the PIC and cabin crew at the point of embarkation. Transit and destination airports also need to be advised that such a person is being carried. The original operator advises all other operators involved in the transport of the inadmissible passenger to their final destination.

The following information is provided to the originating operator, as well as subsequent operators:

- Name and sex of the person identified as the deportee; reason for deportation (nature of crime);
- Willingness or unwillingness to travel by air;
- Whether the person has attempted to escape custody;
- Whether the person has any history of violence;
- Whether the person has a history of self-harm;
- Whether members of the person's family are booked on the same flight;
- Whether the person is likely to be the target of harm during the transportation;
- Identity of escorts (if required);
- The mental and/or physical state of the person;
- Wanted status of the person (by any other authority);
- Other information that would allow an operator to assess the risk of endangering the security of the flight;
- Special conditions and precautions for transport of the person, if any.

To ensure the safety of the aircraft during a flight, an operator typically has a process to assess the information (see above) associated with the transport of passengers that require special attention. For example, a decision might be needed as to whether a passenger will be denied boarding, or whether a passenger might require an escort.

Accordingly, there is usually a well-defined escort policy that is provided to the appropriate immigration authorities. Females travelling under the provisions of a judicial order may require a female escorting officer as a member of the escort team.

Special provisions may exist for flights where transportation of multiple inadmissible passengers is required.

Although a person is involved in travel in response to a judicial or custodial order, while in flight, such passenger is always under the control of the PIC and crew of the aircraft.

3.6 Hold Baggage

SEC 3.6.1

If the Operator conducts international passenger flights, the Operator shall have a process to ensure originating hold baggage, including courier baggage, is:

△

(i) Subjected to screening capable of detecting explosives and explosive devices prior to being loaded into an aircraft for an international passenger flight;

(ii) Protected from unauthorized interference from the moment of acceptance until loaded on board the aircraft. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) for ensuring all originating checked baggage is subjected to screening prior to being loaded onto an aircraft.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** passenger/baggage handling operations (focus: originating hold baggage is subjected to screening prior to being loaded onto an aircraft for an international flight).
- ☐ **Other Actions** (Specify)

Guidance

All checked baggage loaded on international flights is examined by authorized screeners using approved screening methods. Each state will have varying regulations and requirements, but typically approved screening methods include:

- Explosive detection systems (EDS);
- Explosive trace detection (ETD);
- X-ray;
- Physical search;
- Canine.

Where the State delegates screening to the operator, or where the foreign host government does not perform screening to the standard required, the operator is responsible for ensuring all checked baggage is screened to the appropriate level and meets the requirements of the Operator.

In the event of an increased threat, the operator, based on risk assessment, may direct supplementary screening procedures as appropriate to counter the threat.

Courier service is an operation whereby shipments tendered by one or more shippers are transported as the baggage of a courier passenger on board a scheduled airline flight under normal passenger hold baggage documentation.

This provision also refers to a person who is employed by a courier service operator and travels as a passenger or crew member, and who checks a courier shipment in as hold baggage. Such baggage is then screened under the same requirements that apply to all hold baggage.

SEC 3.6.2

If the Operator conducts domestic passenger flights, the Operator should have a process to ensure originating hold baggage is:

△

(i) Subjected to screening capable of detecting explosives and explosive devices prior to being loaded into an aircraft for a domestic passenger flight;

(ii) Protected from unauthorized interference from the moment of acceptance until they are loaded on board the aircraft.

Auditor Actions

- ☐ **Identified/Assessed** process(es) for ensuring all originating checked baggage is subjected to screening prior to being loaded.
- ☐ **Observed** the hold baggage screening process.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** passenger/baggage handling operations (focus: originating hold baggage is subjected to screening prior to being loaded onto an aircraft).
- ☐ **Other Actions** (Specify)

SEC 3.6.3–3.6.5 (Intentionally open)

SEC 3.6.6

If the Operator conducts international passenger flights, the Operator shall have a process to ensure procedures are in place to prevent items of hold baggage from being transported on such flights unless such items have been:

(i) Individually identified as either accompanied or unaccompanied baggage;

(ii) Subjected to appropriate security controls based on risk assessment. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to identify if hold baggage is accompanied or unaccompanied.
- ☐ **Identified** appropriate security controls performed on unaccompanied checked baggage before being transported on international flights.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Observed** passenger/baggage handling operations (focus: process for ensuring passenger-baggage reconciliation for international flights).
- ☐ **Other Actions** (Specify)

Guidance

An operator typically has a system in place to identify a passenger who fails to board a flight after check-in or fails to re-board a flight at a transit stop. In an effort to reduce the risk, the aviation industry initially introduced a system where passengers identified their bags before loading. That system can still be invoked at remote locations if no other procedure exists.

The intent of this provision is for an operator to have a process to verify and confirm, before a flight departs, that only baggage that has been properly identified, screened to the appropriate standard and accepted for carriage has been uplifted.

Applicable primarily to flights operated solely for the purpose of transporting passengers on a charter basis (e.g. executive charters, VIP charters), if permitted by the State, the requirement for passenger baggage reconciliation procedures may be rescinded. Additionally, as permitted by the State, baggage reconciliation procedures could be rescinded:

- For specific passengers designated as VIPs (e.g. heads of state) who are being transported on scheduled passenger flights;
- When baggage and passengers are separated for reasons beyond the control of the passengers (e.g. mishandled bag, involuntary offloading due to an oversold flight, weather diversions, operational aircraft change, passenger re-routing, weight restrictions).

3.7 Cargo Shipments

SEC 3.7.1

If the Operator transports revenue or non-revenue cargo, the Operator shall have a process to ensure cargo shipments for transport on all flights have been subjected to the appropriate security controls, including screening where required, as established by the applicable state(s) prior to being loaded onto an aircraft.

Auditor Actions

- ☐ **Identified/Assessed** process(es) to ensure cargo has been subjected to the appropriate security controls.
- ☐ **Identified/Assessed** process(es) to ensure security controls performed on cargo meet the requirement of the applicable state(s).
- ☐ **Examined** selected records that reflect implementation of cargo security controls.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

3.8 In-Flight, Catering and Other Supplies

SEC 3.8.1

If the Operator conducts passenger flights, the Operator shall have a process to ensure in-flight, catering and/or other supplies intended for transport on a passenger flight are subjected to appropriate security controls as established by the appropriate state and are thereafter protected from unauthorized interference until loaded onto the aircraft. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to secure in-flight, catering and other supplies.
- ☐ **Identified/Assessed** process(es) to ensure all in-flight, catering and other supplies are protected from unauthorized access once security controls have been implemented.
- ☐ **Observed** in-flight, catering and other security controls.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Catering supplies are frequently prepared by an external service provider at an off-airport location.

Additional guidance may be found in the IATA Security Manual.

3.9 General Protection

SEC 3.9.1 (Intentionally open)

SEC 3.9.2

If the Operator controls security restricted areas, the Operator shall have processes to ensure merchandise and supplies introduced into such areas are subject to appropriate security controls, which may include screening or a supply chain security process. **(GM)**

Auditor Actions

- ☐ **Identified** security restricted areas controlled by the operator.
- ☐ **Identified/Assessed** process(es) to secure merchandise/supplies prior to introduction into operator-controlled security restricted areas.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Security Restricted Area.

Protection measures might include sealing, visual monitoring or any other method that will detect or physically prevent unauthorized interference.

An operator would be deemed as controlling a security restricted area when it is the accountable party nominated to ensure the integrity of the sterile area.

4 Security Threat and Contingency Management

4.1 Threat Management

SEC 4.1.1

The Operator shall have processes for maintaining a constant review of the level and nature of security and cybersecurity threats to civil aviation, and for identifying direct or potential threats against the Operator and/or its aircraft operations. For threats that have been identified, such processes shall include:

(i) An assessment of associated risks and vulnerabilities;

(ii) Development of appropriate response measures. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) for monitoring level and nature of security threats to civil aviation (focus: identification of threats to operator, assessment of associated risks, development of response measures).
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** methods used to monitor security threats to civil aviation.
- ☐ **Examined** selected records of threats identified, risk assessments and appropriate response measures.
- ☐ **Other Actions** (Specify)

Guidance

Refer to the IRM for the definition of Cybersecurity.

To ensure threat assessment remains up to date and relevant to the changing environment, an operator will have mechanisms in place that allow it to collect real-time (or close to real-time) security threat information from both open and, if possible, restricted sources. Included would be relevant information shared or provided by applicable states for the purpose of assisting the operator in (1) identifying direct or potential threats to its operations and (2) conducting effective security risk assessments.

Processes would include, based on threat information received, periodic security risk assessment(s), with the focus on airports it operates to, usual flight routes and any locations where it may have assets.

Furthermore, significant security or geo-political events would also be monitored to indicate the possible need for unscheduled security risk assessments and, if applicable, development of appropriate response measures.

Procedures might also include instructions for communicating security threats to persons responsible for making decisions and taking action, as well as providing advice to the flight crew. Means of communication and details of telephone numbers, emergency radio channels and contact persons would be readily available to ensure a response to threats without delay.

An operator's security threat review process will typically include an Aircraft Cyber Risk Assessment Framework (ACRAF) that is implemented and integrated in its risk management framework to ensure:

- Critical systems, information, assets and data (CSIAD) relative to the aircraft are identified;
- Cyber threats relevant to the identified CSIAD are analyzed to determine corresponding risks to aircraft operations;
- Cyber risks are assessed to determine the requirement for risk mitigation action(s).

Risk mitigation actions are an output of the risk assessment process and are implemented in operations. In addition, any risks and vulnerabilities discovered during the process would be reported to the applicable OEMs and other relevant external providers.

An operator typically identifies one senior management official that is accountable for the risk management of cybersecurity operations and has the authority to plan and allocate the resources necessary to manage cybersecurity risks.

Risk management framework preparation step

The aircraft cyber risk assessment is typically established at the aircraft life-cycle operations level. A first preparation step would be consistent with the latest revision of the NIST SP800-37, which ties back to ISO/IEC 27001:2013 and based on (Information Technology Infrastructure Library) ITIL or ISO/IEC 31000 principles. The following would be defined within the operator's risk management framework:

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

Note: *Risk Assessment is normally conducted on a regular basis.*

Identification and categorization of CSIAD step

The identification and categorization of the aircraft CSIAD and interconnected CSIAD, and the information processed, stored, and transmitted, would normally be based on an impact analysis. The categorization via an impact analysis would follow the latest guidance version of FIPS 199 and NIST Special Publications SP 800-30, 800-59, 800-60.

Evaluation of threats against CSID element step

Once the above step is completed, each identified CSIAD element would go through the evaluation of threats against it, the development of the security requirements and the selection of security controls that will protect the element. The security requirements would normally follow the latest guidance version of the NIST Special Publications SP-800-171.

Protection of CSIAD via Security Controls step

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 follow the latest guidance version of FIPS 199 and 200 for minimum security requirements and NIST Special Publications SP 800-30, 800-53 for security control selection guidance for non-national security system. CNSS instruction 1253 can also help support this step for national security systems. Implementation would follow the latest guidance version of the NIST SP 800-53, 800-53A, 800-53B.

Assessment of effectiveness of the selected Security Controls step

After implementation of the selected security controls, the operator would continue to assess cyber threats relative to the CSIAD, determine any residual risks to aircraft operations and determine the need for additional mitigating actions to supplement or replace existing security controls. The assessment activity would typically follow the latest guidance version of NIST SP 800-53A, 800-53B and SP 800-70.

SEC 4.1.2

The Operator shall have a process to ensure the implementation of appropriate security measures in response to:

(i) Security threats directed against the Operator;

(ii) Threat levels issued by applicable aviation security authorities. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** process(es) to implement appropriate security measures in response to any security threats directed against the operator, or threat levels issued by the applicable aviation security authorities.
- ☐ **Observed** implementation of appropriate security measures in response to security threats and threat levels issued by aviation security authorities.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

The contingency plan for response to an increased threat to operations is included in the AOSP.

An assessment of increased threat could come from the authorities or from an operator's own threat assessment process.

Procedures typically set out the increase in security measures appropriate to counter a situation of increased threat, as well as methods used to communicate any changes in threat level to the flight crew, operational personnel, management and overseas stations. There is also normally a verification process to ensure required measures have been implemented without delay.

SEC 4.1.3

The Operator shall have procedures for sharing, as appropriate, with the State, relevant operators, airport authority, air traffic service and external service providers, in a practical and timely manner, relevant information to assist in the implementation of an effective security risk assessment process. **(GM)**

Note: *This provision is applicable to the Operator only if procedures for sharing the specified relevant information are approved by the State.*

Auditor Actions

- ☐ **Identified/Assessed** procedures for sharing relevant security information with the specified entities.
- ☐ **Observed** implementation of appropriate security measures in response to security threats and threat levels issued by aviation security.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records of security information sharing.
- ☐ **Other Actions** (Specify)

Guidance

The information shared typically would include, but not be limited to, geopolitical information at the national and airport level as well as potential flight paths, identified security deficiencies, security inspection and audit results, and security measures implemented.

It is important that the procedures for sharing information are approved by the State and developed according to guidelines established by the State.

4.2 Contingency Planning

SEC 4.2.1

The Operator shall have a contingency plan that provides for a comprehensive and managed response to aviation security incidents. **(GM)**

Auditor Actions

- ☐ **Identified/Assessed** contingency plan.
- ☐ **Reviewed** contents of the contingency plan applicability to aviation security incident responses.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Other Actions** (Specify)

Guidance

The primary objective of a contingency plan is the protection of life and property and the resumption of normal operations. The secondary objective is investigation to determine if the crisis was an accident or a crime; the latter typically requires those found responsible to be taken into custody.

4.3 Investigation and Notification

SEC 4.3.1

The Operator shall have a process to ensure an investigation is conducted for any of the following:

(i) Threats or acts of unlawful interference;

(ii) Failure of implementation of security controls under the responsibility of the Operator;

(iii) Security incidents, security occurrences or security threats. **(GM)**

Auditor Actions

- ☐ **Identified** process(es) to investigate security incidents.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected incident investigation documents and reports.
- ☐ **Other Actions** (Specify)

Guidance

Investigation outcomes may be integrated with root causes identified through the quality assurance program as part of the continuous improvement cycle of the Operator's SeMS.

Refer to the IATA SeMS manual for guidance that addresses the SeMS continuous cycle.

SEC 4.3.2

The Operator shall have a process that ensures notification to the applicable aviation security authorities when an act of unlawful interference against the Operator, a reportable security incident and/or a reportable security occurrence has been identified. **(GM)**

Auditor Actions

- ☐ **Identified** process(es) used to notify applicable aviation security authorities when an act of unlawful interference against the Operator has occurred.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected notifications of acts of unlawful interference.
- ☐ **Other Actions** (Specify)

Guidance

The intent of this provision is for an operator to have procedures in place to immediately notify local security and civil aviation authorities and to provide information relevant to credible threats and acts of unlawful interference. An operator would typically have contact information and checklists readily available for this purpose.

Procedures typically specify an initial verbal notification followed by a written notification.

SEC 4.3.3

The Operator *should* have a process to ensure security incidents and/or security occurrences are reported to IATA for inclusion in the Incident Data Exchange (IDX) Security Dashboard. Such reports *should* be submitted in accordance with the formal IDX reporting process. **(GM)**

Auditor Actions

- ☐ **Identified** process for submission of security information to IATA for the IDX Security Dashboard.
- ☐ **Interviewed** responsible manager(s).
- ☐ **Examined** selected records of information submission.
- ☐ **Other Actions** (Specify)

Guidance

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

IDX has replaced the IATA Safety Trend Evaluation, Analysis and Data Exchange System (STEADES). IDX permits operators to report security incidents and security occurrences for uploading into the IDX security management database and subsequent analysis by users.

To facilitate the reporting of security incidents and security occurrences to IDX, an operator's reporting process could use a taxonomy that is aligned with the IDX security taxonomy, which is called the IATA Safety Incidents Taxonomy (ISIT). Accordingly, an operator would be encouraged to select applicable parent descriptors from the full IDX list and use its own subcategories depending on the operator's scope of operations or specific business requirements. In such case, some descriptors may be applicable whereas others may not.

The specifications in SEC 1.12.1 require an operator to establish a security reporting system covering acts of unlawful interference, security incidents and security occurrences. In the absence of a globally recognized definition, the operator, depending on its scope of operations, is encouraged to identify descriptors that are related to acts of unlawful interference, security incidents and security occurrences.

Reports should be submitted to IATA on a regular basis and include the date and location of security incidents and occurrences (for flight-related reports, this would be a departure airport) as well as a title, a summary and related security descriptors as per the IDX Data Submission Guidelines.