



**Security Management
Systems (SEMS)
for Air Transport Operators
Executive Summary**

July 2007

Security Management Systems (SEMS) for Air Transport Operators

Executive Summary

1. Introduction

- Security Management Systems (SEMS) is a more structured and standardized approach to how Security processes should be implemented and will provide overall better and more uniform standards throughout the aviation industry.
- Implementing SEMS as well as an effective and focused threat assessment process should contribute to making Security processes pro-active.
- Essentially, an SEMS is an element of corporate management's responsibility which sets out a company's Security policy to manage Security as an integral part of its overall business making Security one of the company's core values by developing a Security culture
- SEMS is a business-like approach to Security; goals are set, levels of authority are established, etc. much the same as with Quality Management Systems (QMS) and Safety Management Systems (SMS).
- When viewed in this context it becomes obvious that the three programs (SEMS, QMS, SMS) must be harmonized to ensure consistency and an equivalent level of attention.
- Further, SEMS is based on ICAO Annex 17 standards and the IATA Operational Safety Audit (IOSA) Security Standards. Through IOSA, SEMS already has a Quality Management segment in place. QMS becomes a complimentary system
- Each airline must implement the system that works best in their specific situation – there is no “one-size-fits-all” system.
- The SEMS template should serve as a guide of what should be achieved after full implementation of SEMS.
- In order to have an effective Security Management System, it should include the methods and procedures to achieve:
 - Senior management commitment to Security
 - Appointment of a Head of Security
 - Creation of a Security department organisational structure
 - Promotion of a Security culture
 - Training of Security personnel
 - Security awareness training for all employees
 - Regular evaluation of Security personnel
 - Effective day to day Security operations
 - Incident and accident investigative reporting
 - Continuous correction from the outcome of incident accident investigation report.
 - Threat assessment
 - Risk Management
 - Emergency response procedures
 - Regular audits and protocols for correction of deficiencies
- The following points should be made when a Security Management System is implemented:
 - Companies should build on existing procedures and practices rather than start all over. SEMS should be seen as an evolutionary tool rather than a revolutionary device.
 - Adoption of “best practice” standards must be the goal. The Air Carrier Security Programme requirements mandate the minimum requirement for an air carrier to be

compliant. SEMS will help air carriers achieve “best practice” standards which would be in compliance with requirements of all States where the air carrier operates.

- A SEMS must be a company-wide system. Established at the corporate level, the SEMS should then devolve to individual departments. Flight Operations, In-flight, Baggage Services, Passenger Services, Airport Services, Telephone Sales and all other departments whose activities contribute to Security need to develop their own procedures under the umbrella of the SEMS.
- Each air carrier is responsible for the development of security procedures and operational bulletins based on the concepts of this template taking into account their own operational environment resources available and regulatory framework of their State of registry and State(s) of operations
- If some Security operations are outsourced, contracts should identify the need for equivalent, auditable SEMS in the supplier.
- In order for SEMS to be successful, it needs endorsement from the concerned regulators and all stakeholders involved in aviation.

2. Organization and Management

- There is a need for senior management to formally endorse, in a written document, their commitment to Security as a central component of the air carrier's core values.
- A Head of Security with a direct reporting line to senior management should be appointed
- A clear organizational chart of the Security department should be drafted where all necessary responsibilities have a dedicated point of contact. The organizational chart should be proportionate to the size of the company.
- Security should be every employee's responsibility and should be an integral part of the management plan.
- Communication of Security information, as appropriate, is a very important part of the development of a Security culture.
- When employing contractors the following information should be provided by the contractor to the air carrier before agreeing to use their services:
 - Security arrangement and procedures
 - Previous Security record
 - Hiring and staff training policies
 - A routine audit should be performed
- Further to that the air carrier should submit appropriate sections of the SEMS to the contractor and ensure that they are willing to be in line with the air carrier's Security culture commitment.
- Security documentation and manuals should be centralised and readily accessible to all employees affected by the document or appropriate sections.

3. Human Resources Management

- Procedures should be put in place to hire competent staff and ensure that they have been cleared by background checks as outlined in National legislation, and the air carrier security programme.
- An efficient training programme should be developed for staff involved in implementation of security measures. Effective and measurable initial & recurrent training and testing/evaluation modalities should be developed.
- Security awareness training sessions should be attended by all employees, periodically, in order to promote a Security culture.

- Performance appraisals should be conducted on a regular basis to ensure that all employees perform their functions adequately in a co-operative and constructive manner benefiting both the employer and employee
- Human factors need to be taken into consideration when developing effective Security procedures.
- Human factors should be considered essential in maintaining staff motivation at acceptable levels.
- Staff rotation and work variety contribute in maintaining staff motivation and productivity.

4. Quality Assurance

- In order to ensure that Security measures are in compliance with mandated requirements, quality controls should be put in place.
- Many options exist for quality control measures, both internally and externally, each with their advantages and disadvantages.
- The best approach to ensure quality assurance is most likely a combination of both internal and external quality control measures.
- Further to that, international audit mechanisms such as IOSA and the ICAO Universal Security Audit Programme (USAP) are in place to guarantee acceptable global Security standards. SEMS can help air carriers meet IOSA Security Standards and Recommended Practices. SEMS can also help States, who have endorsed these principles, successfully meet USAP audit requirements.

5. Security Operations

- SEMS should provide details into how to achieve “best practice” Standards for the necessary Security processes to ensure protection of all air carrier assets. Care must be exercised to ensure consistency with National legislation regarding aviation security.
- The topics to be covered in SEMS should include but are not limited to the following:
 - Access Control
 - Perimeter Security
 - Airside Security
 - Protection of parked aircraft
 - Airport personnel identification
 - Aircraft security
 - Pre-flight aircraft searches
 - Reinforced cockpit doors
 - Carriage of weapons
 - Authorise carriage of weapons
 - Carriage of weapons as baggage
 - Passenger, supernumeraries and cabin baggage Security
 - Passenger identity verification
 - Passenger and carry-on baggage screening
 - Transit and transfer passengers
 - Special screening procedures
 - Diplomats
 - Persons exempted from screening
 - Persons in custody and under administrative control
 - Airline crew, airport staff and other non-passenger
 - Monitoring performance of Security equipment

- Hold baggage Security
- Cargo, mail and express parcels Security controls
- Catering and stores Security
- Risk and Threat assessment
- Security Audits
- Accountable Document Security

It is very useful to clearly assign responsibilities between the airlines, airport authorities and other entities involved in maintaining security.

6. Contingencies

- Air carriers should have risk and threat assessment as well as risk and threat management mechanisms developed. Some States offer assistance in the threat assessment process. State mandates should have priority when they are in place.
- Air carriers should have an emergency response plan in place for incidents of all types, including Security incidents. The appropriate infrastructure and staffing should be put in place.
- Emergency measures should exist in the eventuality of at least the following security related incidents which are the most common:
 - Bomb threat
 - Bomb threat against buildings (including provisions for terminal evacuation)
 - Hijacking
- Air carriers can learn a significant amount of information about flaws in their operations when incidents take place. However, it is best to discover flaws through security exercises. In order for incidents to be learning experiences, there needs to be a thorough investigation process that can identify where procedures were lacking in order to remedy and implement corrective action.

7. Additional Security Accountabilities

- Security issues that are important to air carriers, but not necessarily directly related to compliance of the Air Security Programme, may also be included as part of SEMS. This further reiterates that SEMS is designed to be an all encompassing Security document that promotes Security awareness.
- Issues to be addressed as part of organizational extensions can be but are not limited to:
 - Aviation Security related issues:
 - Disruptive passengers
 - Inadmissible passengers
 - Stowaways
 - Passenger risk assessment
 - Protection of layover crew and ex-pat staff
 - Theft
 - Fraud and insider crime
 - Building and infrastructure security
 - International Security Standards and Recommended Practices (Legal framework)
 - Co-operation with airport security and other AVSEC/regulatory agencies
 - Mutual recognition and harmonization of Security requirements and procedures
 - AVSEC roles of station managers