Security Management Systems (SEMS) for Air Transport Operators

Executive Summary

March 2011
Security Management Systems (SeMS) for Air Transport Operators

Executive Summary

Introduction and Scope

In early 2002, the Security Committee requested IATA’s help to draft the Security Management document incorporating both aviation security and corporate security, the recommended security structure for an airline and guidance on the management of security.

Security management system was not designed to impose a complete overhaul of one’s security operations rather it was created to demonstrate what should be aimed for. If current policies and practices within an organization provide a satisfactory outcome, there may not be any need to change or modify the approach.

This executive summary should be used in conjunction with the IATA Security Manual and other tools which provide detailed guidance on the implementation of the various aspects outlined in this document.

Security management systems (SeMS), by integrating security awareness throughout the organization and verifying compliance through quality assurance, can be a significant force in achieving the highest possible level of regulatory compliance. Specific security practices, training and audit functions within a security management system should all be built so as to ensure compliance with applicable national aviation security programmes.

This executive summary is to provide the reader with an overview of security management systems, the elements required to obtain and implement such a system, and a model implementation guide.

Why Security Management Systems?

The aviation industry remains a legitimate target in the eyes of terrorists. The focus of terrorist attacks has changed since 2001 as now casualties are a central part of terrorist operations rather than simply be collateral damage.

Since 2001, every organization involved in air transportation has re-assessed and is still re-assessing their security measures.

The ultimate goal of the Security Management System is to serve as a guideline for IATA’s member airlines in helping them build effective aviation security measures. A standardized structure, such as SeMS, provides better and more uniform security standards throughout the airline industry. Through implementation of SeMS an effective and focused threat assessment should contribute to making security practices proactive instead of relying on more traditional reactive procedures.
What is a Security Management System?

A Security Management System is an element of the corporate management responsibility which sets out a company's security policies and its intent to manage security as an integral part of its overall business. It is important to keep in mind however that each airline must implement the system that works best in their specific situation – there is no “one-size-fits-all” system.

A SeMS is a businesslike approach to security. As with any business plan, goals are set, levels of authority are established and so on.

Ultimately, SeMS becomes woven into the fabric of the organization and becomes part of its culture.

Core Elements

In order to have and effective Security Management System, it should include the following Core Elements and sub-elements. As there is no “one-size-fits-all”, each airline may choose to group or break down these elements and sub-elements in different ways, in accordance with their own security management system structure, but the each objective of the elements are met:

- **Senior Management Commitment**
  - Head of Security
  - Security Department Organization

- **Resource Management**
  - Staff Selection
  - Staff Evaluation
  - Security Training Program
  - Security Awareness
  - Management of Service Providers

- **Threat Assessment & Risk Management**
  - Identification of threats and risks
  - Threat Assessment
  - Risk Assessment

- **Management of Emergency & Incidents (Resilience)**
  - Emergency Preparedness & Response
  - Crisis & Contingency Management Plans
  - Security Incident Management

- **Quality Control & Quality Assurance**
  - Corrective Action mechanism
  - External Service Providers

- **Aviation Security Program**
  - Document Procedures
Understanding the Core Elements

Senior Management Commitment

No matter the size, type or complexity of operations, senior management of the parent company as well as the top executive of the organization play a major role in determining a company’s commitment to security. General directions and visions should come from the senior management at the highest level. They are responsible for setting the security standards and promoting security within the organization.

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

The head of security is generally assigned responsibility for:
- Formulation of an overall security policy for senior management acceptance;
- The development and promulgation of security standards and practices to provide line management with direction and control;
- Establishing a clear order of command in the security structure;
- Ensuring effectiveness of security program by regular evaluation and inspection;
- Effective liaison with governments, authorities and law enforcement agencies;
- Ensuring an effective risk analysis, threat assessment and response capability;
- Initiating special security measures during periods/instances of increased threat;

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.

Communication of security information, as appropriate, is a very important part of the senior management commitment.

Resource 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 program. An efficient training program should be developed for staff involved in implementation of security measures. Effective and measurable initial and recurrent training and testing/evaluation modalities should be developed. Security awareness training session 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 cooperative and constructive manner benefiting both the employer and the employee.

Procedures should also be put in place for service providers regarding selection, security training and awareness.
**Threat Assessment and Risk Management**

Air carriers should identify the threats and risks their organization is exposed to as a first step. The nature of the threats will then be evaluated as well as their likelihood and consequence which could render the organization at risk. The risk assessment is then used to address risks consistently and transparently; to protect staff, assets and brand; to prioritize resource allocation; and to serve as an early warning system. The assessment of risk also enables the operator to measure security performance against measures contained in the airline and airport security programs.

Some States offer assistance in the threat assessment process. State mandates should have priority when they are in place.

IATA has developed a Risk Assessment Template which IATA member airlines could refer to (available by IATA upon request).

**Management of Emergency and Incidents (Resilience)**

Public confidence is imperative in commercial air transportation. Although statistically, air travel is the safest mode of transportation, the fact is that air travel accidents usually involve massive loss of life, human suffering and hull loss which contribute to damaging public confidence for the industry as a whole. Failure to act accordingly during, and even after an incident will directly impact the affected organization.

Air carriers should ensure that procedures are in place to handle security-related incidents and avoid operations being disrupted from them. Security-related incidents should be reported, investigated and managed.

Standards should be in place to ensure that the Operator has suitable crisis and contingency management plans in place, which are implemented and tested, which address any breaches of security likely to result in an act of unlawful interference in relation to its operations, the response to changes in threat level or any other relevant disruption.

For security incidents likely to result in an act of unlawful interference or expose the operator to vulnerability, a timely and comprehensive investigation is necessary.

**Quality Control and Quality Assurance**

Quality control and quality assurance are undertaken in order to review and assess procedures and processes, in place within the organization, are with desired security outcomes.

The organization shall have a process in place for conducting periodic or event-driven security surveys which identify the needs and weaknesses of the Security Program, including operational security procedures and infrastructure.

The organization shall also have a quality assurance program that provides for the auditing and evaluation of the management system and operational security functions at planned intervals to ensure it is complying with the Security Program, achieving the Security Program objectives; and properly applying security standards.
Many options exist for quality control measures, both internally and externally, each with their advantages and disadvantages.

Mechanisms shall also be put in place for addressing the findings under quality control and quality assurance which describe the necessary actions and time frames towards addressing the findings.

The organization must ensure that their external service providers carry out functions and responsibilities consistent with contractual agreements and host state regulatory requirements.

**Aviation Security Program**

The air carrier should have a formal Security Program that includes the requirements of the civil aviation security program of the State, the applicable requirements of other states where operations are conducted and the security policy and standards of the Operator. The Security Program is required in order to:

- Protect customers, personnel and assets from any act of unlawful interference or related unlawful act;
- Provide directions on security measures required;
- Comply with regulatory requirements

The Security Program provides a structure for security policy and awareness, which flows from senior management to all levels of operational personnel within the organization. The documented Security Program, as a minimum, specifies or makes reference to other documents that specify:

- Airline security policy and objectives;
- Means for achieving these objectives including establishing a security department;
- Structure and responsibilities of the security department;
- Security responsibilities of operational personnel, handling agents and other contractors;
- Minimum and contingency protective measures;
- Risk analysis, threat assessment and counter measures.

In addition to stating responsibilities of the designated head of security, the Security Program specifies responsibilities of other personnel that perform operational security functions within the organization.

Security issues which are important to air carriers, but not necessarily directly related to compliance of the Security Program, may also be included in the SeMS. This further reiterates that SeMS is designed to be an all encompassing security document that promotes security awareness. It is not meant however to replace the Security Program.

---

1 Such issues can be: Disruptive passengers, inadmissible passengers, stowaways, protection of layover crew, theft, fraud and insider crime, building and infrastructure security, cooperation with airport security and other AVSEC regulatory agencies, aviation security roles of station managers, etc.
Understanding a Security Management System

When establishing a security management system, organizations should build on existing procedures and practices rather than starting from an empty sheet – or rather starting all over. The adoption of “best practice” standards must be the goal in the process.

A security management system is company wide, established at the corporate level, the SeMS should then devolve to individual departments; Flight operations, in-flight, baggage services, passenger service, airport services, and all other departments whose activities contribute to security need to develop their own procedures under the umbrella of security management systems.

Each air carrier is responsible for the development of security procedures and operational bulletins based the core elements, taking into account their own operational environment resources available and regulatory framework of their State of Registry and State(s) of operation.

If some security operations are outsourced, contract should identify the need for equivalent, auditable SeMS in the supplier.

Implementing a Security Management System – A Model Plan

When an organization decides that it will implement a security management system in their operations, it is essential that a plan is drawn out.

The implementation of SeMS is complex and involves a great number of entities within and outside of the organization. It is paramount that all affected parties are aware of what is expected of them, who they will need to co-operate with and at which moment in the project. Clearly the size and scope is very dependent many variables including the size of the organization, the current level of integration, regulatory requirements, etc.

A model SEMS implementation plan is included in Table 1 below. Only high level activities are mentioned. When an organization decides to implement SEMS, it will need to identify each individual task, under all the main project components, detail them and provide a timeline. Multiple tasks can and should be undertaken at the same time. However, some tasks will be dependent on the outcomes of other. For large organizations the number of line items can easily be in the hundreds.
TABLE 1: Model SEMS Implementation Plan

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Duration</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEMS Project</td>
<td>6 months - 2 years</td>
<td>Need to track all monthly status meeting reports and working sessions.</td>
</tr>
<tr>
<td>Project Management</td>
<td>6 months - 2 years</td>
<td>Long time due to the scale and scope of the project and required senior management approval and endorsements.</td>
</tr>
<tr>
<td>Project Charter</td>
<td>2 weeks - 3 months</td>
<td>Provide regular updates to civil aviation authority on progress. Gain provisional guidance to ensure compliance to the regulatory requirements.</td>
</tr>
<tr>
<td>Presentations to Civil Aviation Authority</td>
<td>Ongoing ~ duration of project</td>
<td>When no regulatory requirement for SEMS exist, it can be difficult to determine what is necessary. In the case where there are no regulatory requirements, it will necessary to use baseline standards to measure against. IOSA Security standards can be used. Once the requirements are known a gap analysis will have to be performed against the set requirements.</td>
</tr>
<tr>
<td>Regulation and Standards</td>
<td>1 week - 1 month</td>
<td>Project team will conduct an &quot;audit&quot; of their business unit determining if the Core Element as defined was Documented, Implemented and Controlled. If an element is not documented but implemented or partially, (most of the time) it can therefore not be Controlled. The gap analysis will determine the amount of work needed to be done and also identify areas where it is possible to leverage current processes.</td>
</tr>
<tr>
<td>Kick-off Meeting</td>
<td>1 week - 1 month</td>
<td>Meeting Preparation should be included.</td>
</tr>
<tr>
<td>Document Current State (Documented, Implemented and Controlled within Core Elements)</td>
<td>2 weeks - 3 months</td>
<td>Corporate Security policy review process but also review of policies that can be affected by security.</td>
</tr>
<tr>
<td>Task Name</td>
<td>Duration</td>
<td>Guidelines</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organizational Structure</td>
<td>1 week - 4 months</td>
<td>Determine the infrastructure required to implement and sustain SEMS.</td>
</tr>
<tr>
<td>Job Competencies</td>
<td>2 weeks - 6 months</td>
<td>Documentation of all management functions, including the process and ownership to sustain and manage once documented.</td>
</tr>
<tr>
<td>Integrated Business Processes</td>
<td>1 month - 6 months</td>
<td>Documentation of a common process for all entities to follow ensuring continuity and when trending, comparing similar reports. If possible a Corporate standard for reporting activities in all disciplines should be established.</td>
</tr>
<tr>
<td>SEMS Project - IT Solution</td>
<td>0 days - 2 years</td>
<td>Develop an IT system to manage and sustain all that processes developed. This is normally one of the largest task with the longest timeline.</td>
</tr>
<tr>
<td>Communication</td>
<td>Ongoing - duration of project</td>
<td>Tracking of the communication plan / strategy</td>
</tr>
<tr>
<td>SEMS Quality Manual</td>
<td>2 months - 1 year</td>
<td>Documenting a Quality Manual documenting all of the Corporate standards and processes in response to SEMS and regulatory or baseline requirements. This may be incorporated within existing manuals depending on the size and complexity of the organization.</td>
</tr>
<tr>
<td>Risk Model</td>
<td>2 months - 1 year</td>
<td>Documenting a Corporate Risk model to ensure all reports are managed in the same manner.</td>
</tr>
<tr>
<td>Security Incident Reporting Mechanism</td>
<td>1 month - 1 year</td>
<td>Documentation of process to support written policy, ensuring fair and equal treatment. Need to consider and get approvals from unions, associations, third party contractors, etc.</td>
</tr>
<tr>
<td>Security Committees</td>
<td>2 weeks - 4 months</td>
<td>Documentation of all Security team/committee meetings, including attendees, mandate, authority, hierarchy, etc.</td>
</tr>
<tr>
<td>Company-wide Audit Programme</td>
<td>2 weeks - 4 months</td>
<td>Normally, not required but does contribute to decrease costs if there is an integrated audit plan developed that cross-utilize resources.</td>
</tr>
<tr>
<td>SEMS Training</td>
<td>Ongoing - duration of project</td>
<td>Develop and track all training required for SEMS readiness. Very important component to ensure compliance.</td>
</tr>
</tbody>
</table>
### SEMS High-Level Implementation Project Plan (Model)

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Duration</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal SEMS audit</td>
<td>1 month - 6 months</td>
<td>Internal audit in preparation of Regulator assessment. Should Include usage of assessment questions to be used and unbiased auditors conducting the audit, documenting findings and allowing time for corrective actions.</td>
</tr>
<tr>
<td>SEMS Submission to Regulator for Approval</td>
<td>Dependant on Regulator requirements and timelines</td>
<td>Tracking of compliance process. Can include the final assessment of the Organisation's SEMS.</td>
</tr>
<tr>
<td>Project Closure</td>
<td>2 weeks - 3 months</td>
<td>Administrative, project management issues. Timeline dependant on complexity and length of project.</td>
</tr>
</tbody>
</table>

Please note that the timelines indicated are guidance only and will be dependant on the size and complexity of the organization. It can take anywhere from 6 months for a small carrier up to 2 years for a legacy carrier to implement SeMS. As with any project, the dedication and commitment of resources are critical to ensuring timelines are met and adhered to.

### Benefits of Security Management Systems

A Security Management System allows each organization to achieve the same goal in a way that's appropriate to their business model. SeMS also provides the flexibility to achieve outcomes in a way that can be tailored to individual operations and to change as business models change.
Next Steps

IATA is developing a Security Management Systems Implementation Guide for Air Transport Operators which will be available in October 2011.

For further information please contact: secfal@iata.org