International Civil Aviation Organization
Latin American Civil Aviation Commission
ICAO/LACAC NAM/CAR/SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG)

WORKING PAPER

AVSEC/FAL/RG/5 — WP/08
28/05/15

FIFTH MEETING OF THE AVIATION SECURITY AND FACILITATION REGIONAL GROUP (AVSEC/FAL/RG/5)

ICAO SAM Regional Office, Lima, Peru, 3 to 5 June 2015

Agenda Item 4: **Programmes and Projects – Aviation Security (AVSEC)**
4.2 Report on *Aviation Security Management Systems* programme – Coordinator State Colombia

RESULTS OF THE MEETING ON AVIATION SECURITY MANAGEMENT SYSTEM (SeMS)

(Presented by Argentina, Colombia, Cuba, Costa Rica, Honduras and Mexico)

EXECUTIVE SUMMARY	
Presentation of the results obtained during the Aviation Security Management Systems (SeMS) Working Meeting held in Buenos Aires, Argentina from 12 to 15 May 2015.	
Action:	Suggested actions are detailed in paragraph 3) of this working paper.
Strategic Objectives:	• Security & Facilitation
References:	• Chicago Convention • Annex 9 – Facilitation • Annex 17 – Security • Annex 19 – Safety Management • Doc. 8973/9 • Doc. 9734 Parte C • Doc. 9735 • Doc. 9808 • Doc. 9859 • AVSEC/FAL/RG/4 Final Report • AVSECP/26 Final Report

1. Introduction

1.1 In the Fourth Meeting of the Aviation Security and Facilitation Regional Group held in Mexico City, Mexico, from 3 to 5 June 2014, Argentina presented WP/15, stating the possibility of developing a study on the implementation of an Aviation Security Management System (SeMS), from a

regional perspective. The experiences of some States were discussed, highlighting the problems related to SeMS implementation.

1.2 During this discussion the risk analysis problematic was considered, which required appropriate coordination with the different Government entities that could lead to a duplication of responsibilities, the problematic to obtain information of the operators with regard to their deficiencies was also considered.

1.3 Finally, the Regional Group concluded, during the Fourth Meeting, on the need to make a greater assessment on this issue, proposing and convening in the creation of a Task Force, leaded by Colombia, to carry out such assessment.

1.4 During 2014, the AVSEC/FAL Regional Group Secretariat proposed organizing a working meeting to achieve the task assigned, assess the activities so far developed, plan the needs of the Region and prepare a schedule according to such needs.

1.5 The AVSEC authority of the Republic of Argentina, responding to the Secretariat proposal, acted as host for the development of the working meeting, which took place in the *Centro de Instrucción, Perfeccionamiento y Experimentación (CIPE)*, Buenos Aires, Argentina, from 12 to 15 May 2015. As a result of the meeting, the following considerations, complemented by the information attached in **Appendix A,** emerged.

2. Analysis

2.1 During the meeting in Buenos Aires, it was proposed to understand the need and/or convenience of implementing a SeMS, identify its components and compare its concepts with those of a Safety Management System (SMS) in the scope of their interrelation, and generate a guide for the States that would like to participate of the pilot implementation of a SeMS.

2.2 In order to comply with the proposed objective for the meeting, the existing documentation regarding SeMS and SMS was analyzed. In addition, the working meeting took note of the modification of Doc. 8973 “Security Manual” ninth edition, presented by the Working Group on Guidance Material to the ASEC Panel, during their 26th meeting, carried out in ICAO HQ from 13 to 17 April 2015, and worked on a non-official translation into Spanish of this document, which for ease of reference is attached as **Appendix B** to this working paper.

2.3 Making a more in depth analysis of the above mentioned technical documents, they are considered of great usefulness to conduct the work, which is considered an important progress in the eventual standardization of a monitoring system, which enables to ensure the quality of the components of an aviation security system.

2.4 From the experience shared, some aeronautical operators have started to implement a SeMS within the management system, without the States and/or corresponding authority intervention, generating an essential flow of information, which could benefit the international civil aviation protection system and the global system itself. Notwithstanding, the absence of specific standards and technical guidance in the material prepared by the corresponding authority, makes it impossible to take advantage of these continuous monitoring management systems, and can even generate distorsions in the accomplishment of current standards due to the absence of a standard framework that allows interactivity.

2.5 In addition, the Task Force counted on the presence of a specialist in the implementation of a State Safety Programme (SSP)/Safety Management System (SMS), to consider the experience in the

implementation of a SSP/SMS, in order to use the common points in the development and implementation of both systems.

2.6 Finally, the participants of the meeting provided and shared their knowledge and experience, which result in the following conclusions:

- The implementation of SeMS is appropriate in the organizations that provide services affecting civil aviation security, such as air operators, accredited cargo agents, private security companies, ground service providers, State security, etc.
- Some principles of SeMS are common with SMS, however, there are differential characteristics between each that make essential the individual development of SeMS implementation considering the particularities or differences of the indicators, such as Hazard and Threat and the management of such processes.
- The application of SeMS should not leave aside that communications should be made in the framework of confidentiality of information and limited distribution, usual of the indicators used for the work in civil aviation protection.
- The implementation of a management system requires the adoption of commitments and responsibilities with specific references in order to strengthen the concepts related to the authority of the manager in charge, both within the corresponding State authority and operators involved. In this regard, the benefit of making a planning of the referred stages, proposing the Region to limit the experimental implementation to the processes being jointly developed, such as the security procedures for passenger and baggage control points, as well as to limit the application to the participation of the corresponding authority, air operators and airport managers during the first phases of the implementation.

3. Suggested action

3.1 The Meeting is invited to analyze this working paper and its appendices, exchange criteria and suggest the pertinent measures.

3.2 To submit for consideration of the States the continuation of the SeMS Working Group in order to take note and report to the AVSEC/FAL/RG the progress that interested States have reached in SeMS implementation.

— — — — — — — — — — —

APPENDIX A

Security Management System (SeMS)

Applying a Systems Security Management (SeMS), provides the AVSEC authority of the State and operators with responsibilities assigned in aviation security, a structured approach to managing security as part of AVSEC focus on a integral system. Also, the application of a SeMS is useful as a tool for the systematic integration of risk management of aviation safety and operations on a day-to-day in close alignment with other management systems.

The study of the subject has shown that the application of a SeMS not based on the creation of new responsibilities, but in the awareness of how the measures apply and are managed the human and material resources in order to comply efficiently the current responsibilities

In this sense, the first step of a SeMS is to recognize all the system components that make up the civil aviation of the state, as well as activities associated to these components, such as those quality control tasks, instruction and certification, approval of programs, risk management, etc. Thus, once identified the components, should emphasize the following principles of SeMS:

- Management commitment;
- Resources;
- Threat and risk management;
- Performance monitoring, reporting and continuous improvement;
- Incident response;
- SeMS training programme;
- Communication.

The establishment of a SeMS requires the express designation of those responsible for its implementation and detail of their own tasks.

1. AUTHORITIES:

Accountable executive:

The Contracting State, administrations of airports and air operators (although this is limited to other service providers or agencies with responsibilities in compliance with the National Civil Aviation Security Programme), should incorporate the functions of the maximum authority of that organization, corresponding to an accountable executive.

Security Manager:

The authorities or agencies mentioned in the previous paragraph, should designate as Manager Aviation Security an appropriately qualified person and with experience in aviation security, considering the size, structure and complexity of such agencies or authorities.

2. RESPONSIBILITIES:

Accountable executive:

Accountable executive, who may have more than one function within their organization, should be ultimately responsible and accountable for the effective implementation of security within entities. They should have the appropriate level of authority within their organization to allocate resources necessary in the implementation of efficient and effective SeMS.

The role of the accountable executive is to foster security as a core organizational value, ensure that the SeMS is properly implemented and maintained through the allocation of resources and tasks. Accountable executives should therefore be responsible for the development and effectiveness of SeMS, and be granted with the following:

- Responsibility for determining the level of risk that the entity can tolerate (in the case of the AVSEC authority, for industry must adjust management to meet the risk policy established by the state);
- Corporate authority for ensuring that all activities can be financed and adequately staffed;
- Final accountability for all security issues;
- Responsibility to ensure that all staff understand the entity's security policy;
- Fully support and engender a security culture throughout the organisation.

Security Manager:

To assist the accountable executive in his duties, and taking into consideration the size and complexity of entities, specific tasks should be delegated to a security manager who remains independent of other managers within the organization. Security managers should be the focal point for all SeMS matters and be responsible for managing, administering and maintaining SeMS.

Security Manager is responsible for:

- Implement training and awareness to achieve a strong security culture in the organization;
- Incorporate activities of the organization dynamic and proactive approach established by the Accountable Executive;
- Identify, manage and mitigate security risks consistently and proactively;
- Focus on performance, results and impacts;
- Monitor activities based on the level of threat determined by the authority;
- Effectively implementing the internal and external partnerships, collaboration and cooperation.

Such tasks may include, but are not limited to, managing security reporting systems, maintaining documentation and training records, providing input to the development of training material, participating in security investigations, and providing advice and reports to the accountable executive and other executives as appropriate.

Security managers should be qualified to appropriate national standards as well as possessing the following skills:

- Practical experience of and expertise in the entity's operations;
- Knowledge of security and quality management;
- Knowledge of the entity's security programme;
- Thorough understanding of the aviation security requirements applicable to the entity.

3. DOCUMENTATION:

The agencies or authorities must develop a written management plan to ensure integral quality of civil aviation security, built-in security programs (NCASP - ASP) designed for qualitative evaluation to improve the effectiveness of SeMS requirements and security measures continuously.

The performance indicators of the security management system (including all processes and quality control, risk management, certification, training, etc.) must be identified in order to monitor the effective implementation of aviation security requirements, providing all management indicators with a precise level image of effectiveness of SeMS.

Management planning incorporated into the security program must allow the agencies / authorities to monitor and measure all aspects of SeMS, and include the following:

- Definition of performance requirements and indicators for all security measures of international civil aviation;
- Conducting risk assessments and impact before to the implementation of new measures and / or modified in situations of structural change;
- Collection and analysis of data necessary to demonstrate the adequacy of the security systems and mitigation measures;
- Review active measures after an increase in cases or security reports;
- Review of the elements and procedures of a particular specific operation;
- Management security data and information of limited distribution to make sure it is protected from unauthorized interference;
- Assessments of facilities, equipment and documentation;
- Staff performance in order to verify compliance with the responsibilities and skills required in aviation security for each individual;
- Implementation of corrective measures to address the security deficiencies identified during quality control activities.

— END —

APPENDIX B

AVIATION SECURITY MANAGEMENT SECURITY SYSTEMS

(text to replace 9.2 Security Management System Safety Manual)

1. General

1.1 Security management systems (SeMS) provide entities with a structured approach to managing security as an integral part of its overall business. SeMS serve as a tool for systematically integrating security risk management into an entities day-to-day operation in close alignment with other risk management systems.

1.2 SeMS are designed to be integrated with, or connected to, other structured management systems such as a Safety Management System (SMS) or quality management system, whilst also incorporating relevant parts of any informal management system. Other management systems serve as a foundation for SeMS, thus minimizing duplication and expense while contributing to an entity's business capability and credibility.

1.3 States that intend to adopt and implement a SeMS, or elements thereof, should make use of the guidance below in guiding the entities responsible for implementing aviation security (e.g. aircraft operators, airport operators and regulated agents) in the delivery of such an approach.

1.4 States should adapt their NQCP to ensure the effective oversight of SeMS, or elements thereof, as implemented by entities.

An oversight system

1.5 SeMS are an organized, systematic approach to managing aviation security. Whilst a 'security culture' encourages optimal security performance within entities, SeMS are assurance systems that provide those entities the necessary organizational structure, accountabilities, policies and procedures to ensure effective oversight of their security operations.

1.6 SeMS typically ensure key risks are effectively identified, mitigated and subject to regular review. SeMS are therefore considered an efficient tool to continuously and efficiently assess the effectiveness of aviation security measures in a proactive manner.

Objectives and benefits

1.7 The implementation of SeMS should therefore enable entities to:

a) promote strong security culture;

b) foster a dynamic and risk-based approach to security;

c) effectively identify, manage and mitigate security risks in a consistent and proactive manner;

d) focus on performance, results and impacts;

e) allow oversight to become increasingly risk-based and data-driven; and

f) promote effective internal and external partnerships, collaboration and cooperation.

Documentation

1.8 Information related to the implementation of SeMS, including policies, procedures and responsibilities should be readily accessible to all personnel. Entities should develop a SeMS manual or similar document that consolidates all relevant information.

1.9 The SeMS manual may be a standalone document or simply part of entities' security programmes. Should it be a standalone document, entities should ensure that it includes an index of its existing documents, systems, security policies and records for ease of reference.

Key components

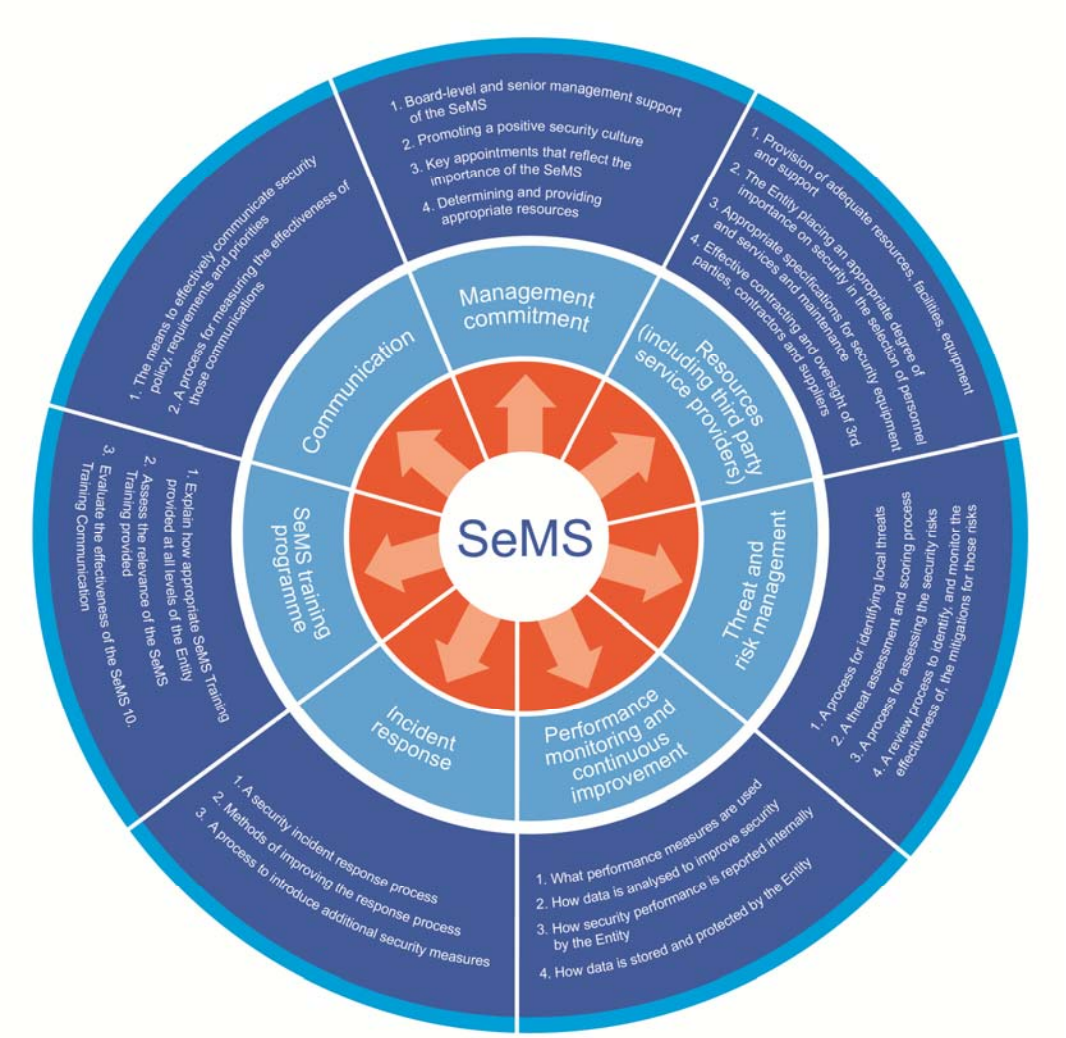

Figure 1-9. SeMS key components

1.10 SeMS should include the following key components (see figure 9-1) applicable to entities responsible for implementing aviation security measures, or any entity playing a role in the safeguarding of civil aviation against acts of unlawful interference:

a) management commitment;

b) resources (including third party service providers);

c) threat and risk management;

d) performance monitoring, reporting and continuous improvement;

e) incident response;

f) SeMS training programme; and

g) communication.

2. Management commitment

2.1 Entities should ensure that full commitment of every level of leadership, from top management to supervisors, is applied at all times and in all activities, strategies, policies and objectives to continuously improve security culture. In this regard, quality assurance programmes such as SeMS can be an efficient tool in keeping management and personnel alert and committed to security culture principles.

2.2 Where SeMS has been adopted, it can be used to engender and promote an effective security culture within entities.

Accountable executive and security managers

2.3 Entities should appoint an accountable executive at the senior executive level, ideally the Chief Executive Officer of the entity concerned or a suitably qualified individual taking into account the size, structure and complexity of those entities. Accountable executive, who may have more than one function within their organization, should be ultimately responsible and accountable for the effective implementation of security within entities. They should have the appropriate level of authority within their organization to allocate resources necessary in the implementation of efficient and effective SeMS.

2.4 The role of the accountable executive is to foster security as a core organizational value, ensure that the SeMS is properly implemented and maintained through the allocation of resources and tasks. Accountable executives should therefore be responsible for the development and effectiveness of SeMS, and be granted with the following:

a) full accountability for the SeMS;

b) responsibility for determining the level of risk that the entity can tolerate;

c) corporate authority for ensuring that all activities can be financed and adequately staffed;

d) final accountability for all security issues;

e) responsibility to ensure that all staff understand the entity’s security policy; and

f) fully support and engender a security culture throughout the organisation.

2.5 To assist the accountable executive in his duties, and taking into consideration the size and complexity of entities, specific tasks should be delegated to a security manager who remains independent of other managers within the organization. Security managers should be the focal point for all SeMS matters and be responsible for managing, administering and maintaining SeMS.

2.6 Such tasks may include, but are not limited to, managing security reporting systems, maintaining documentation and training records, providing input to the development of training material, participating in security investigations, and providing advice and reports to the accountable executive and other executives as appropriate.

2.7 Security managers should be qualified to appropriate national standards as well as possessing the following skills:

a) practical experience of and expertise in the entity's operations;

b) knowledge of security and quality management;

c) knowledge of the entity's security programme; and

d) thorough understanding of the aviation security requirements applicable to the entity.

Governance mechanism

2.8 Governance mechanisms are typically in the form of executive or advisory groups, within which several entities with common security goals and operating in coordination with each other are equally consulted (e.g. airport, aircraft operators and local government agencies carrying out security duties at that same airport, could form a security executive group fulfilling the governance responsibilities).

2.9 Accountable executives should ensure that an effective governance mechanism and structure is in place to address all matters pertaining to security and assist in the following tasks:

a) monitor overall security outcomes against the entity's security policy and objectives;

b) monitor the effectiveness of the entity's operational security processes;

c) ensure that required corrective and/or preventative actions are implemented in a timely fashion; and

d) ensure that the correct resources are correctly/adequately allocated to achieve the security outcomes and level of performance sought by the entity.

3. Resources

3.1 Accountable executives should ensure that the appropriate resources that their entities need in order to efficiently and effectively implement and maintain the SeMS and associated security requirements and processes are provided. Such resources should include personnel, facilities, equipment and supporting services, and be sufficient, suitable and appropriately maintained to achieve security outcomes.

3.2 Security personnel should be recruited, vetted and trained in accordance with the requirements set out in SeMS and other applicable aviation security programmes such as the NCASTP. Training records and performance evaluations should be maintained accordingly and as defined in SeMS.

3.3 More information on recruitment, selection and training can be found in Chapter 8.

Third party service providers

3.4 When entities employ third party service providers (i.e. contracted entities, which may also be entities implementing their own SeMS) for aviation security purposes, the ultimate responsibility for any product or service provided by the contracted entities remains with the contracting entity. Consequently, the effective provisions of such security services should be monitored by the contracting entities, and security requirements should be included in their respective SeMS.

3.5 Entities should clearly define security requirements to be fulfilled by third parties and share security information accordingly and where appropriate to do so, including changes in the threat environment or national security requirements as required by appropriate authorities.

4. Threat and risk assessment

4.1 As detailed earlier in this Chapter, States and relevant national authorities should carry out periodic threat and risk assessments at a national level, taking into account international, national and regional situations and environments. From these assessments, mitigating measures that industry stakeholders (i.e. organizations and entities responsible for implementing aviation security measures, or playing a role in the safeguarding of civil aviation against acts of unlawful interference) are responsible for implementing and/or complying with, are developed.

4.2 In addition, entities implementing SeMS should develop and carry out a local threat identification process supplementing the national threat and risk assessments, in coordination with other local parties involved, be it local stakeholders (e.g. aircraft operators and airport security providers) or government agencies (e.g. border protection, police agencies and air traffic service providers).

4.3 When entities identify threats, they should determine whether the risks associated with the threats should lead to changes in security frameworks. Such assessments should be periodically carried out in order to ensure the effectiveness of the measures in place in accordance with the threat.

4.4 More information on threat and risk assessment can be found in Chapter 9.

Management of change in threat and operational environment

4.5 Changes in threat environment (e.g. the occurrence of security incidents or an increase in national security threat level) may require the urgent application of additional security measures or, when no other alternatives exist at that particular point in time, the suspension of operations. SeMS should include processes to quickly and adequately address the need for the urgent application of additional security measures resulting from a change in the threat environment.

4.6 Entities should establish a documented process that identifies internal or external changes that may have an impact on security. Those changes may be engendered by, for example, changes in the threat environment, States' security requirements, and internal policy. Further information on contingency

planning can be found in Chapter 17. Such a process should take into account how the following may be impacted by changes:

a) critical systems and activities;

b) stability of systems and operational environments; and

c) past performance.

5. Performance monitoring, reporting, and continuous improvement

5.1 Entities should develop quality assurance programmes designed to qualitatively assess and continuously improve the effectiveness of SeMS requirements and security measures in place. Security performance indicators should be identified with a view to monitoring the effective implementation of aviation security requirements, and thus providing all levels of management with an accurate picture of the level of effectiveness of SeMS.

5.2 Quality assurance programmes should enable entities to monitor and measure all aspects of SeMS, and include the following elements:

a) defining performance requirements and metrics for all aviation security measures;

b) conducting risk and impact assessments prior to the implementation of new and/or modified measures, or in situations of structural change;

c) collecting and analysing data to demonstrate the suitability of security systems and mitigation measures;

d) reviewing active measures following an increase in incidents or security reports;

e) reviewing particular elements or procedures of a specific operation;

f) management of security data and information to ensure it is protected from unauthorized interference;

g) assessments of facilities, equipment and documentation;

h) personnel performance in order to verify the fulfilment of each individual’s security responsibilities;

i) conducting security audits focusing on the integrity of SeMS;

j) conducting internal investigations of security occurrences; and

k) conducting security tests.

Assessment, corrective and preventative actions

5.3 Following the collection and analysis of security data in accordance with SeMS and quality assurance programme, entities should identify the cause of unsatisfactory performance, if applicable, and

develop a corrective action plan to remedy such performance, prevent recurrence and continuously improve SeMS and security systems as a whole.

5.4 Entities should document the procedures in place designed to assist in the following tasks:

a) reviewing unsatisfactory performance;

b) determining the causal factors of unsatisfactory performance, which may be related to:

i) training;

ii) equipment performance;

iii) policy;

iv) procedures; and

v) human factors;

c) evaluating the need for effective and purposeful actions to ensure that unsatisfactory performance is mitigated;

d) determining, implementing and recording the appropriate corrective or preventative actions; and

e) reviewing any actions taken.

Security reporting system

5.5 The objective of a security reporting system is to collect information as reported by personnel to improve the level of security performance. It should assist in identifying deficiencies, incidents or unsatisfactory performance, and aim to encourage individuals to report incidents and deficiencies that would otherwise remain unnoticed and would therefore not be corrected.

5.6 More information on reporting systems can be found in Chapter 9.

Sharing of information

5.7 Entities, including appropriate authorities, should collaborate on the development of new security management approaches, techniques and tools to assist other entities in their efforts to assess and improve the effectiveness of their security systems. For example, information on best practices should be disseminated as widely as possible.

6. Incident response

6.1 SeMS should include procedures and processes to be carried out in response to security incidents. The SeMS incident response framework should be reviewed regularly to ensure they remain commensurate with incidents already encountered, and appropriate to future incidents which may differ in nature with past events. Where appropriate, entities should coordinate incident response processes and procedures with those of other entities involved.

6.2 The incident response framework included in the SeMS should be designed to assist entities in improving their security measures and systems following an incident or exercise (table-top or drill). Continuous improvement may thus be achieved by conducting a review and analysis of the relevant parts of the incident response process after each exercise or incident.

7. SeMS training programme

7.1 In order to achieve an effective and efficient implementation of SeMS, all relevant personnel should possess appropriate skills and be trained according to the needs established by SeMS, to ensure they are competent to perform their duties and fulfil their responsibilities.

7.2 Entities should develop and maintain a SeMS training programme to be delivered to all personnel concerned by the implementation of SeMS (i.e. all levels of management including operational personnel, supervisors, senior managers, accountable executives and security managers). Such a training programme should be commensurate and appropriate to the personnel's responsibility and level of involvement in SeMS, and its effectiveness should be regularly reviewed.

7.3 SeMS training programmes should ensure that:

a) senior managers fully understand their security responsibilities and accountabilities;

b) all personnel are trained and remain competent to perform their relevant SeMS duties;

c) all personnel receive basic training in security awareness where required; and

d) the effectiveness of training and education provided to personnel is regularly measured.

7.4 More information on recruitment, selection and training can be found in Chapter 8. Information on background check can be found in Chapter 11.

8. Communication

8.1 Similar to internal and external communication guidelines recommended in the application of security culture, entities should establish a formal means of communicating the requirements, policy and any relevant information pertaining to SeMS to all relevant personnel. Such means should also describe the role that security committees play in communicating and sharing security information, both within entities, and across other entities when applicable.

8.2 Communication mechanisms should aim to:

a) ensure that all personnel are fully aware of their duties, as well as the reporting mechanisms in place in the entity;

b) ensure that all relevant personnel are fully aware of the SeMS and its requirements;

c) convey security-critical information in line with relevant restrictions (SASI);

d) inform about the rationale behind the implementation of, or changes to particular security procedures.

Communication tools

8.3 Entities should make best use of available resources, media and fora such as regular meetings, security awareness training, intranet, newsletters, security bulletins and SeMS documentation.

8.4 More information on communication and security awareness campaigns can be found in Chapter 9.

— END —