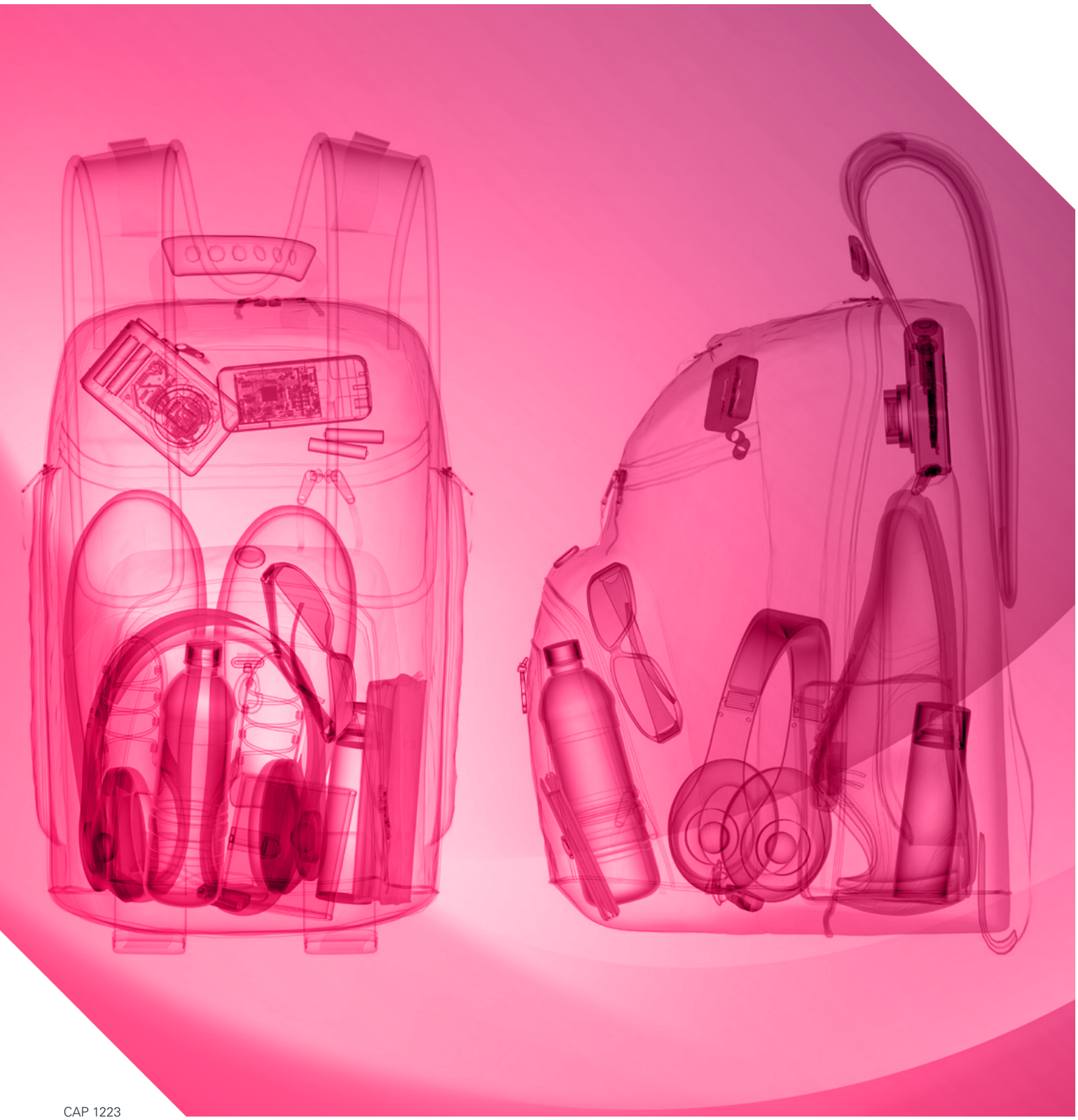
Department for Transport

Civil Aviation Authority

# Framework for an Aviation Security Management System (SeMS)



CAP 1223

CAA House, 45-59 Kingsway, London WC2B 6TE
www.caa.co.uk

# Contents

# Definitions

**Accountable Manager** – The Accountable Manager is the senior person within the Entity who is ultimately responsible and accountable for the delivery of security within that Entity. The role is described in more detail in Chapter 1 of this document.

**Aviation Security Requirements** – Aviation Security Requirements is a reference to the EU aviation security common basic standards and the more stringent measures applied in the UK.

**Entity** – The Entity is the Airport Operator, Air Carrier, Regulated Agent, In-Flight Supplier or any other organisation engaged in delivering aviation security.

**Relevant Personnel** – Where in this document reference is made to Relevant Personnel the Entity should specify, within its SeMS, who the relevant personnel are in each context.

**Security Manager** – The Security Manager is the subject matter expert whom the Accountable Manager directs to implement and maintain the SeMS and then who uses the SeMS to provide assurance to the Entity.

**SeMS** – A SeMS is an organised, systematic approach to managing security which embeds security management into the day to day activities of an organisation. It provides the necessary organisational structure, accountabilities, policies and procedures to ensure effective oversight. In summary, a SeMS is an assurance system for security.

**SeMS Manual** – A SeMS Manual is a manual or a collection of existing materials, or a combination of both, which describes how the Entity will deliver its SeMS.

**SeMS Training** – SeMS Training is a reference to training to enable the Entity to operate an effective SeMS and any additional training identified by the Entity to deliver its security processes.

# Introduction

1. **The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation**
2. **In order for a SeMS to be effective it should have the components described in this framework**

## Purpose

A SeMS provides a formalised, risk-driven framework for integrating security into the daily operations and culture of an Entity. The SeMS enables an Entity to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way. A SeMS is not a mandated process but if an Entity has a SeMS which contains all the elements which are identified in this framework, it will help the Entity to meet the internal quality control provisions of articles 12, 13 and 14 of EC 300/2008[1].

## Implementation

A SeMS Manual need not be a separate document. Many of the components will already exist in an Entity's security programme, operational processes, operating procedures or other documents. In order to have a security management system, an Entity only needs to include in its SeMS Manual an index or map of its existing documents, systems and records.

Depending on its size and complexity, an Entity may decide to combine its security policy, security programme and SeMS Manual into a single document or to keep them separate as complementary documents.

Whatever form the SeMS Manual may take the SeMS itself should be part of the Entity's overall management system.

## SeMS philosophy

The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.

In order for a SeMS to be effective (for both industry and the CAA) it should include the components set out in this document.

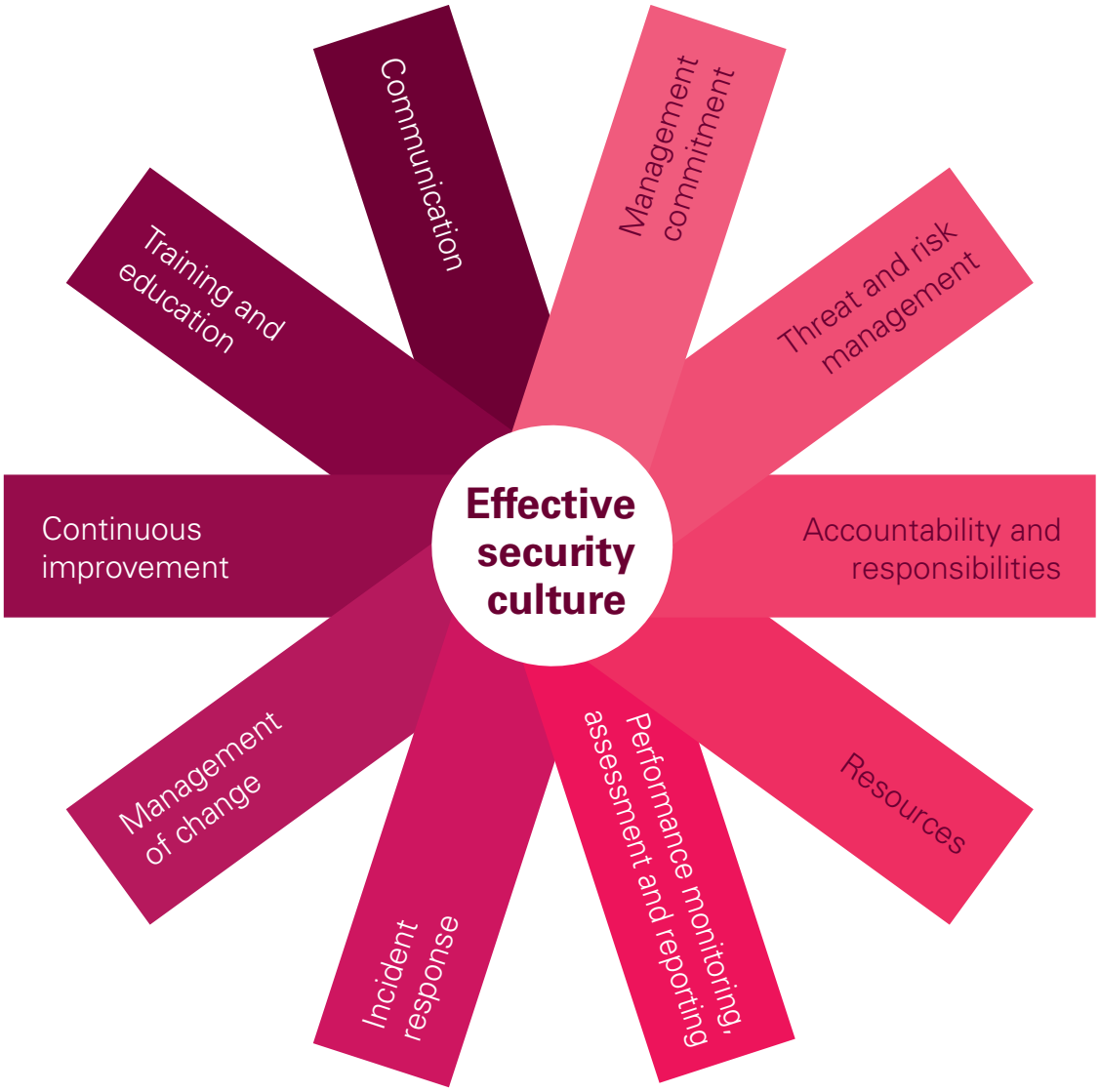
1 Regulation (EC) 300/2008 of the European Parliament and of the Council of 11 March 2008.

## Key components of a SeMS

A SeMS should include the following key components applicable to all types and sizes of aviation Entity:

1. Management commitment
2. Threat and risk management
3. Accountability and responsibilities
4. Resources
5. Performance monitoring, assessment and reporting
6. Incident response
7. Management of change
8. Continuous improvement
9. Training and education
10. Communication

Chapters 1 to 10 cover each of these components in turn.



CHAPTER 1

# Management commitment

**The Entity's management should show its commitment to security by:**

1. **Board-level and senior management support of the SeMS**
2. **Promoting a positive security culture**
3. **Key appointments that reflect the importance of the SeMS**
4. **Determining and providing the appropriate resources**

## Senior management commitment

Senior management should:

- promote the Entity's security policy to all personnel and demonstrate their commitment to it;
- establish the Entity's security objectives and performance standards; and
- determine and provide the necessary human and financial resources for the SeMS.

## Security policy statement

The security policy is the means whereby the Entity states its intention to maintain and, where practicable, improve security levels in all its activities.

The security policy should:

- be endorsed by the Accountable Manager;
- identify security as a high organisational priority mutually supportive of commercial and operational priorities;
- reflect organisational commitments regarding security and the Entity's proactive and systematic management;
- be communicated, with visible endorsement, throughout the Entity;
- include security reporting principles;
- be periodically reviewed to ensure it remains relevant and appropriate to the Entity;

- include a commitment to:
  a) a continuous improvement programme;
  b) ensure Aviation Security Requirements and all applicable standards are met, and consider best practices;
  c) provide appropriate resources;
  d) enforce security as the responsibility of all personnel;
- include security reporting procedures (including access to the Anti-Terrorist hotline) and whistleblowing arrangements; and
- promote a positive security culture.

## Key appointments

The Entity's management should ensure the following key roles are filled with suitably qualified and skilled individuals.

### Accountable Manager

The Accountable Manager's role is to instil security as a core organisational value and to ensure that the SeMS is properly implemented and maintained through the allocation of resources and tasks.

The Accountable Manager may have more than one function in the Entity but should have sufficient authority to be able to direct both finance and resource to the security operation.

The Accountable Manager should be the Chief Executive Officer (CEO) of the Entity or a suitably competent and qualified person appointed by the CEO, taking into account the size, structure and complexity of the Entity.

The Accountable Manager should have a thorough knowledge and understanding of the key issues of risk management within the Entity.

The Accountable Manager's technical knowledge and understanding of SeMS should be sufficient to perform the Accountable Manager role. The Accountable Manager need not know about all the detail of security processes within the Entity but should have an understanding of how the Entity's assurance of the regime is maintained.

Depending on the size and complexity of operations, the Accountable Manager may delegate specified tasks. However, accountability and responsibility for those tasks remains with the Accountable Manager.

### Security Manager

The Security Manager should be the focal point for SeMS and should be tasked with managing the development, administration and maintenance of an effective SeMS. The Security Manager should:

- facilitate threat identification, risk analysis, and management;
- monitor the implementation and functioning of the security management system, including any security actions that the Entity considers necessary;
- manage the security reporting system of the Entity;
- provide periodic assurance reports on security performance to the Entity's Accountable Manager and Board;
- ensure maintenance of security management documentation;
- ensure that security management training that the Entity considers necessary to implement its security operation and its SeMS, is available;
- provide advice on security matters to the Entity; and
- participate in internal occurrence/security investigations.

The Security Manager should have:

- practical experience of and expertise in the Entity's operations;
- knowledge of security and quality management;
- knowledge of the Entity's security programme; and
- comprehensive knowledge of the Aviation Security Requirements applicable to the Entity.

The Security Manager may be any suitably competent and qualified person at appropriate management level, provided that that person can act independently of other managers within the Entity, and has direct access to the Accountable Manager and to appropriate management personnel to raise security matters.

CHAPTER 2

# Threat and risk management

**The SeMS should provide:**

1. **A process for identifying local threats**
2. **A threat assessment and scoring process**
3. **A process for assessing the security risks**
4. **A review process to identify, and monitor the effectiveness of, the mitigations for those risks**

## Local threat identification process

National and international threats are notified to the Entity by the Government and mitigated by regulatory measures. The Entity's threat identification process should supplement this information with a list of locally-identified threats suitably defined and assessed for subsequent use in risk assessment.

When conducting risk and threat assessments Entities are encouraged, where appropriate, to adopt a multi-agency approach as airports currently do. For further information please see the guidance referenced below:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/11516/guide.pdf

## Assessing vulnerabilities

The threat and risk assessment process should capture a clear and comprehensive picture of where vulnerabilities may exist. Only by establishing where vulnerabilities lie can adequate mitigation be considered and assessed.

## Assessing risks

Following assessment of each vulnerability and threat faced by the Entity, the actual risk of such an event occurring and succeeding should be assessed by the Entity.

Security risk assessment is the analysis of the security risks of the consequences of the threats that have been determined.

Security risk analysis breaks down the risks into two components: the probability of occurrence of a damaging event or condition and the severity of the event or condition. Security risk decision making and acceptance should be specified by the Entity through a risk tolerability matrix.

## Review process

The risk register and the mitigations arising from it should be reviewed by the Entity on a regular basis and as and when the threat situation changes.

A formal security risk assessment and mitigation process should be developed and maintained by the Entity that ensures analysis (in terms of probability and severity of occurrence), assessment (in terms of tolerability) and control (in terms of mitigation) of risks.

The frequency of review should depend on local context such as the size or complexity of the operation.

CHAPTER 3

# Accountability and responsibilities

**The SeMS should include:**

1. **Clearly defined accountability and responsibility for security throughout the Entity**
2. **Clearly defined governance arrangements that ensure security is accorded sufficient priority and management attention**

## Defined accountability and responsibilities

The Entity should define accountability and responsibilities for security throughout the Entity, including security governance responsibilities at all levels.

## Security governance mechanisms

The Accountable Manager should put in place governance arrangements that provide the Entity's management with assurance that the SeMS is effective.

The governance mechanism should consider matters of strategic security in support of the Accountable Manager's security accountability. It should:

- monitor security performance against the Entity's security policy and objectives;
- monitor the effectiveness of the Entity's operational security and its security management processes;

- ensure that any security action is taken in a timely manner; and
- ensure that appropriate resources are allocated to achieve the Entity's intended security performance.

Depending on the size of the Entity and the type and complexity of its operations, existing governance structures may be extended to incorporate these governance responsibilities. For example, airports maintain a multi-agency Security Executive Group (SEG)[2] and Risk Advisory Group (RAG)[3], which, with regard to airports, could fulfil the governance responsibilities described[4].

Other Entities are encouraged to adopt a similar approach where appropriate.

2 The Security Executive Group (SEG) brings together people who have the authority to take decisions about the security measures that should be put in place. It includes senior representatives from the airport operator, the local police force, the local police authority and airlines operating at the airport.

3 A Risk Advisory Group (RAG) brings together security practitioners at the airport, including representatives of the airport manager and local chief officer of police. The RAG's function is to produce a Risk Report, assessing each threat to the security of the airport. The RAG then makes recommendations about the security measures that should be taken, or continue to be taken.

4 Guidance on SEG and RAG can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/11516/guide.pdf

**CHAPTER 4**

# Resources

**The SeMS depends on:**

1. **Provision of adequate resources, facilities, equipment and support**
2. **The Entity placing an appropriate degree of importance on security in the selection of personnel**
3. **Appropriate specifications for security equipment and services and maintenance**
4. **Effective contracting and oversight of 3rd parties, contractors and suppliers**

## Provision of resources, facilities, equipment and supporting services

The Entity should determine and provide the appropriate resources that it needs to:

- implement and maintain the SeMS; and
- implement and maintain the security processes that deliver the SeMS, the Aviation Security Requirements and any other risk mitigation identified.

Personnel contributing to a security process should be competent and have appropriate education, training, skills and experience.

The facilities, equipment and supporting services provided should be sufficient, suitable and maintained to achieve the security outcomes, including the Aviation Security Requirements.

The Entity should keep records of these resources for security management and performance reporting purposes as defined in its SeMS.

## Personnel competences for the SeMS

The Entity should provide adequate resources for planned tasks by:

- determining the required competences and qualifications for each role;
- stressing, for appointments to senior roles, the importance the Entity places on security; and
- providing suitably qualified personnel.

## Management of third party suppliers

The ultimate security responsibility for any product or service provided to the Entity by contracted entities remains with the Entity.

The Entity should define responsibilities within its own organisation for managing contracted security activities, including quality assurance of what the 3rd party is providing.

The contracted activities should be included in the Entity's SeMS.

## Receiving third party services

Where the Entity is receiving a 3rd party service which could affect aviation security, it should, where possible, specify any security-related requirements, including the provision of information, to enable the Entity to assure security performance.

## Providing third party services

Where the Entity is providing a 3rd party service to another Entity which could affect aviation security, information should, where possible, be shared with that Entity to provide assurance of security performance.

**CHAPTER 5**

# Performance monitoring, assessment and reporting

**The SeMS should include:**

1. **What performance measures are used**
2. **How data is analysed to improve security**
3. **How security performance is reported internally by the Entity**
4. **How data is stored and protected by the Entity**

## Performance monitoring and measurement process

The Entity should use performance monitoring and measurement to verify its performance of the security processes against the Aviation Security Requirements and the Entity's security policy, objectives, identified risks and specified mitigation measures.

This process should include the setting of security performance indicators and security performance targets and the measurement of the security performance against them.

Security key performance indicators should be identified to inform all levels of relevant management in the Entity.

The performance monitoring and measurement process should include:

- addressing the performance in relation to the Aviation Security Requirements;
- security reviews including trends reviews which are conducted during introduction and deployment of new technologies, change or implementation of procedures, or in situations of structural change, or to explore an increase in incidents or security reports;
- security audits which focus on the integrity of the management system;
- examination of particular elements or procedures of a specific operation; and
- internal security investigations of security incidents.

## Analysis of data

The Entity should determine, collect and analyse appropriate data to demonstrate the suitability of security processes and to evaluate where improvement of the effectiveness of the security processes can be made. This should include data generated as a result of monitoring and measurement and may include data from external sources.

## Corrective action

The Entity should take action to eliminate the cause of poor performance in order to prevent recurrence.

Any corrective actions should be appropriate to deal with the effects of the poor performance identified by the Entity.

A documented procedure should be established to define requirements for:

- reviewing poor performance;
- determining the causes of poor performance;
- evaluating the need for action to ensure that poor performance does not recur;
- determining, implementing and recording the appropriate action; and
- reviewing corrective action taken.

## Preventive action

The Entity should determine action to eliminate the causes of potential poor performance in order to prevent their occurrence. Preventive actions should be proportionate to the effects of the potential poor performance.

A documented procedure should be established to:

- determine potential poor performance and its causes;
- evaluate the need for action to prevent occurrence of poor performance;
- determine, implement and record the appropriate action; and
- review preventive action taken.

## Management of security data and information

The objective for management of security data and information should be to ensure the security of data and information received and used so that it is protected from interference, and access to it is restricted only to those authorised.

## Security reporting system

The overall purpose of the security reporting system is to use reported information to improve the level of security performance and not to attribute blame.

The objectives of the security reporting system should be to:

- enable an assessment to be made of the security implications of each relevant occurrence and serious incident, including previous similar events, so that any appropriate action can be initiated; and
- ensure that knowledge of relevant occurrences and serious incidents is disseminated both internally and externally, where appropriate, so that others may learn from them.

The Entity should identify which events are to be reported.

The security reporting system should have the capability to confirm receipt to the reporter, where appropriate.

The reporting process should be simple and clearly defined including details as to what, how, where and when to report.

Regardless of the source or method of reporting, once the information is received, it should be stored in a manner suitable for easy retrieval and analysis.

Access to the submitted reports should be restricted to protect the identity of the source, where appropriate.

The security reporting system should include a feedback system to the reporting person on the outcome of the occurrence analysis.

The security reporting system should also include a voluntary confidential reporting process for reporting security matters.

## Record keeping

The system used by the Entity for record keeping should provide adequate procedures for storage and backup. The system should ensure records are traceable, retrievable and accessible.

The system should include safeguards to ensure the confidentiality, integrity and availability of the information is maintained.

## Quality assurance of data and information

The quality of security-related data and information should be assured by a quality management system that controls the origination, production, storage, handling, processing, transfer and distribution of that data and information.

CHAPTER 6

# Incident response

**The SeMS should include:**

1. **A security incident response process**
2. **Methods of improving the response process**
3. **A process to introduce additional security measures**

## Incident response

The SeMS should include response processes for dealing with security incidents. The processes should be exercised or reviewed as appropriate on a regular basis.

## Incident response process

The incident response process within the SeMS should ensure continuous improvement. Continuous improvement may, amongst other means, be obtained by:

- conducting a review of the relevant parts of the incident response process after a full or partial exercise;
- debriefing and analysing the response actions after an incident; and
- developing new incident procedures or systems as part of the incident response process when new threats are identified by the SeMS.

Where appropriate, the Entity should co-ordinate its incident response processes with those of other interfacing organisations.

## Initiating special security measures

Changing threat information or a security incident may require the urgent application of additional security measures or the suspension of operations.

The Entity should have a process for the urgent application of such additional security measures or suspension of operations.

CHAPTER 7

# Management of change

**The SeMS should:**

1. **Effectively plan, communicate and implement changes to security policy and procedures**
2. **Monitor and measure the effects of change on security**

## General principles

The Entity should manage the security risks related to a change. The management of change should be a documented process to identify external and internal change that may have an effect on security.

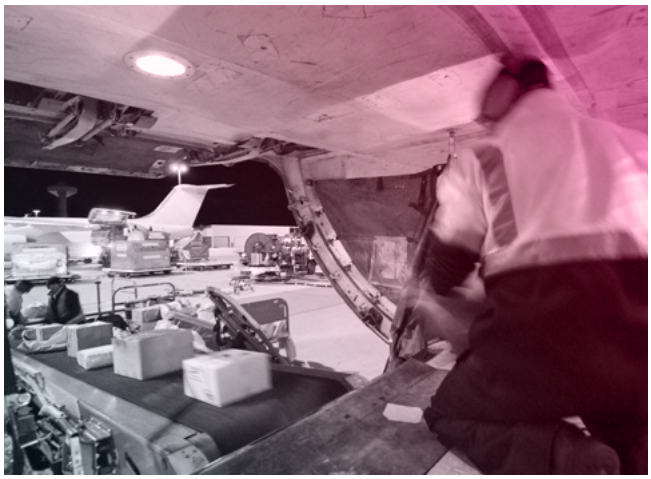
## The management of change

Change can introduce new risks and impact the appropriateness and/or effectiveness of existing risk mitigation strategies. Changes may be external or internal to the Entity.

The Entity should establish a formal process for the management of change which takes into account:

- the criticality of systems and activities;
- the stability of systems and operational environments; and
- past performance.

When changes are planned the Entity should consider any impact on its SeMS.



**CHAPTER 8**

# Continuous improvement

**The SeMS should:**

1. **Seek to improve security performance**
2. **Evaluate all aspects of security provision**
3. **Where appropriate, share security knowledge and skills**

## Continuous improvement

The Entity should seek to improve its security performance through proactive and/or reactive evaluation of the efficiency and effectiveness of:

- the Entity's security procedures;
- the Entity's facilities, equipment and documentation;
- individual performance in the Entity, to verify the fulfilment of each individual's security responsibilities; and
- the Entity's system for control and mitigation of security risks.

Where possible, data relating to the above points should be part of the evaluation.

Similarly the Entity should seek to improve its SeMS, as part of its security assurance, through actions such as:

- internal evaluations;
- independent audits (both internal and external);
- strict document controls; and
- continuous monitoring of security controls and mitigation actions.

## Sharing of information

Whilst aviation has mechanisms for sharing information on safety and on areas of weakness, this is not always the case in the area of security.

The Department for Transport and Civil Aviation Authority will encourage industry to bring forward ideas that lead to a greater sharing of information in ways that do not compromise the effectiveness of security or sensitive information.

In particular, industry will be encouraged to collaborate on the development of new security management approaches, techniques and tools to assist in every Entity's continuous improvement.

**CHAPTER 9**

# SeMS Training and education

**The SeMS should:**

1. **Explain how appropriate SeMS Training will be provided at all levels of the Entity**
2. **Assess the relevance of the SeMS Training provided**
3. **Evaluate the effectiveness of the SeMS Training**

## Aims and scope of training and education

SeMS Training includes high-level awareness of SeMS, education in the concepts and principles of SeMS and detailed training in the processes and procedures of SeMS.

SeMS Training should be relevant to:

- security assurance;
- security promotion;
- security roles and responsibilities; and
- establishing acceptable levels of security.

The Entity should establish a training programme for all personnel, including all levels of management within the Entity (e.g. supervisors, managers, senior managers and the Accountable Manager), and ensure that the effectiveness of the SeMS Training is evaluated.

The amount and level of detail of SeMS Training should be proportionate and appropriate to the individual's responsibility and involvement in the SeMS.

## SeMS Training for the Entity's personnel

### Operational personnel

The SeMS Training should address security responsibilities, including adherence to all operating and security procedures, and recognising and reporting threats.

The training objectives should include the Entity's security policy and should ensure understanding of the Entity's SeMS.

The contents of the SeMS training should, at a level of detail appropriate to the role, include:

- definition of threats;
- consequences and risks;
- the SeMS process, including roles and responsibilities; and
- security reporting and the Entity's security reporting system(s).

### Managers and supervisors

SeMS Training should address security responsibilities, including promoting the SeMS and engaging operational personnel in threat and incident reporting.

In addition to the training objectives established for operational personnel, training objectives for managers and supervisors should include a detailed knowledge of the security process, threat identification and security risk management and mitigation, and change management.

In addition to the contents specified for operational personnel, the training contents for supervisors and managers should also include security data analysis.

### Senior managers

SeMS Training should include security responsibilities in relation to Aviation Security Requirements, as well as the Entity's own security requirements, allocation of resources, ensuring effective internal security communication, and active promotion of the SeMS.

### Accountable Manager

The SeMS Training should provide the Accountable Manager with a general awareness of the Entity's SeMS, including SeMS roles and responsibilities, security policy and objectives, security risk management and security assurance.

CHAPTER 10

# Communication

**The SeMS should describe:**

1. **The means to effectively communicate security policy, requirements and priorities**
2. **A process for measuring the effectiveness of those communications**

## Security communication

The Entity should communicate the SeMS objectives and procedures to all relevant persons and organisations. The SeMS and its application should be evident in all aspects of the Entity's operations.

Security communication should aim to:

- ensure that personnel are aware of the wider security responsibilities shared by all;
- ensure that all Relevant Personnel are fully aware of the SeMS;
- convey security-critical information;
- explain why particular actions are taken; and
- explain why security procedures are introduced or changed.

There should be a process for measuring or assessing the effectiveness of the security communications.

## Communication tools

The Entity may use the following tools to communicate security information:

- the SeMS Manual;
- security processes and procedures;
- security newsletters, notices and bulletins; and
- websites or emails.

Communications should observe protective security markings and dissemination guidance.

Regular meetings with personnel where information, actions and procedures are discussed may also be used to communicate security matters.

Further copies of this publication can be downloaded from **www.caa.co.uk**