Department for Transport

UK Civil Aviation Authority

Framework for an Aviation Security Management System (SeMS)

CAP 1223

Published by the Civil Aviation Authority, 2025

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published 2014
Second edition 2018
Third edition 2021
Fourth edition 2024
Fifth edition 2025

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP1223

Contents

Definitions

SeMS Accountable Manager –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 –Is a reference to the UK National Aviation Security programme (NASP).

Entity – Refers to the Airport Operator, Air Carrier, Regulated Agent, In Flight Supplier, or Known Consignor which owns the SeMS.

Human Factors – is a reference to the application of knowledge about human beings, including their abilities, characteristics and limitations, to the design of the equipment they use, the environments and processes in which they function, and jobs the tasks they perform.

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

Security Management System (SeMS)- Places security at the core of the organisation's operation, integrating it into processes and activities to proactively identify and manage security risks. An effective SeMS provides enhanced security, operational efficiencies and stakeholder engagement fostering a positive security culture.

SeMS Manager-. Is the assigned subject matter expert who implements, maintains, and uses data driven strategies to provide security assurance to the entity. The SeMS Manager will report to the Accountable Manager

SeMS Manual –Is an instruction booklet and/or a collection of existing materials, which describes how the Entity will deliver its SeMS. It is not a requirement under SeMS, but an entity may find it helpful to have one.

Security Education –Refers to education undertaken by all personnel to enable the Entity to operate an effective SeMS. Security Education is there to improve security awareness, promote a positive Security Culture and support any additional training.

Security Culture –Is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organisation and are reflected by the actions and behaviours of both internal and external stakeholders within the organisation.

Security Policy Statement - Is a document describing the importance of security across the organisation. It is used to communicate board level commitment to a robust security model, identify accountabilities and allows the Entity to document its intention to maintain and, where practicable, improve security levels in all its activities.

Security Programme –Describes the methods and procedures which are to be followed by an Entity to comply with the National Aviation Security Programme. The programme should include internal quality control provisions describing how compliance with these methods and procedures are to be monitored by the Entity.

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.**

Note: This revision of the SeMS Framework builds on experience gained since the operational launch of SeMS and incorporates Key Points advice for Entities.

Purpose

SeMS provides a formalised, risk-driven framework for integrating security into the daily operations and culture of an Entity. A SeMS enables an Entity to identify and address security threats, risks, gaps and weaknesses in a consistent and proactive way. Developing a SeMS in line with the elements set out in this framework will assist the Entity to meet the UK quality assurance obligations under our regulatory requirements.

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 Framework.

Security Culture

Security Culture is a set of norms, values, attitudes and assumptions that are inherent in the daily operation of an organisation and are reflected in the actions and behaviours demonstrated by its employees.

A positive Security Culture is the bedrock of an effective SeMS and enables the SeMS to fully deliver its core principles. Each entity, as part of their regulatory requirements, must ensure that there is a present internal policy relating to Security Culture. In addition, it is recommended that Security Culture be regularly monitored and there are many useful materials available which can assist with this such as the UK CAA Security Culture Self-Assessment toolkit. Links to this document can be found in the further guidance section of this framework document.

Entities should consider how the operation of their SeMS contributes to the development of a robust and resilient Security Culture, and how it can positively influence change in actions and/or behaviours that are desirable.

There is no one place that Security Culture sits within the SeMS framework - in fact, it cuts across all 10 chapters, with each having a key role to play. It is crucial that each chapter is reflective in how it positively impacts on Security Culture as the SeMS develops and is embedded across the organisation.

Human factors

Human Factors concerns the application of knowledge about human beings, including their abilities, characteristics and limitations, to the design of the equipment they use, the environments and processes in which they function, and jobs the tasks they perform.

It is closely linked to the concept of human performance, which is the human contribution to system performance and refers to how people perform their work.

The application of Human Factor knowledge is the foundation to a robust security culture and fundamentally informs thew risk management by entities through their SeMS. Decision making, in combination or without technology must be supported by a working environment that allows people to perform to their best, taking their capabilities and limitations into consideration.

As with Security Culture, Human Factors is embedded throughout the 10 chapters of this framework, reflecting the role human performance plays in risk management.

Implementation

We strongly encourage Entities to exploit and enhance their existing systems, processes and governance as they develop their SeMS. Each Entity’s SeMS should be uniquely tailored to suit their business and should form part of the Entity’s overall management system.

An Entity may choose to create a SeMS manual or index to signpost to the relevant security documentation, processes, systems and records. It may include the security programme and the security policy.

It is recognised that SMS and SeMS are closely aligned. Both are underpinned by the principles of Risk Management and should run harmoniously in parallel. Processes may be integrated to ensure efficiency and reduce operating costs.

Entities are encouraged to collaborate with other SeMS Entities/SeMS working groups. This is an opportunity to network and share best practice which will benefit both the organisation and the wider aviation sector.

Key Components of a SeMS

A SeMS should include the following key components:

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. Security Education
10. Communication

Further Guidance

The following publications provide guidance on how to develop a SeMS.

- Guidance for Accountable Managers: https://www.caa.co.uk/cap1224
- Implementing a SeMS: https://www.caa.co.uk/cap1273
- SeMS Guidance for Small Organisations: https://www.caa.co.uk/cap1997
- Security Culture self-assessment tool: https://www.caa.co.uk/Commercial-industry/Security/Security-management-systems/Security-culture-self-assessment-tool/

Key points

1. Ensure governance and resource is allocated to enable the successful maintenance and continuous improvement of SeMS.
2. Placing security information into one manual has its advantages, however, there is no need to reorganise existing documents, procedures, etc. if they support a SeMS, provided clear cross-referencing is applied.
3. An embedded positive Security Culture is the bedrock of an effective SeMS.
4. The application of Human Factors principles is fundamental to risk management in aviation security.
5. Collation and effective use of data driven strategies are essential for managing risks and promoting continuous improvement

Chapter 1

Management commitment

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

1. **Actively demonstrating Board-Level and Senior Management support for the SeMS**
2. **Promoting and embedding a positive Security Culture**
3. **Making key appointments to reflect the importance of the SeMS**
4. **Determining and providing the appropriate resources**

Senior Manager Commitment

Senior managers should:

- promote the Entity's security policy and Security Culture to all personnel and demonstrate their personal 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

SeMS encourage entities to have a security policy statement. This is a written document created by the Entity, setting out its intention to maintain and improve its security levels in all its activities.

The security policy statement should:

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

- include a commitment to:
  a) a continuous improvement programme;
  b) ensuring 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 and inclusive Security Culture.

Key Appointments

Managers should ensure the following key roles are filled with suitably qualified and skilled individuals.

SeMS 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 should:

- hold appropriate authority and accountability within the Entity. This is likely to be an individual at Board or Senior Executive level who has overall responsibility at corporate level for the functions which are subject to aviation security regulation:
- possess thorough knowledge and understanding of the key issues of risk management within the Entity:

  have sufficient technical knowledge and understanding of SeMS to perform the Accountable Manager role: they do not require in-depth knowledge of the Entity's security processes but should understand how the Entity maintains the assurance of its SeMS:

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

More details on the role of an Accountable Manager can be found within CAP 1224 - Guidance Notes for Accountable Managers (https://www.caa.co.uk/cap1224).

SeMS Manager

The SeMS Manager's role is to act as the focal point for SeMS and to manage the development, administration, and maintenance of the Entity's SeMS.

The SeMS Manager should:

- have practical experience of, and expertise in, the Entity's security operations and be able to facilitate threat identification, risk assessment, and risk management;
- monitor the implementation and functioning of the SeMS, including any security actions that the Entity considers necessary;
- conduct effective quality assurance, provide security performance reports to the Accountable Manager and Board
- manage the security reporting system of the Entity;
- ensure maintenance of security management documentation;
- ensure the relevant security management training is in place and conducted to support SeMS and the wider security operation,
- provide advice on security matters to the Entity,
- participate in internal occurrence/security investigations
- have knowledge of the Entity's security programme; and
- comprehensive knowledge of the Aviation Security Requirements applicable to the Entity.

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

Key points

1. It is vital that senior management commit to SeMS at the outset and provide sustained support to the process as it is developed.
2. Ensure that adequate and appropriately skilled resource is provided for SeMS development and, wherever possible, this resource is not diverted to other tasks.
3. The Security Policy should be focused, rooted in SeMS principles, visible and shared with all staff so that it becomes ingrained in the culture.

Chapter 2

Threat and riskmanagement

A SeMS should provide:

1. **A process for identifying local threats**
2. **A threat assessment & 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 threat and risk assessments Entities are encouraged, where appropriate, to adopt a multi-agency approach.

Assessing Vulnerabilities

The threat and risk assessment process should capture a clear and comprehensive picture of where vulnerabilities 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 that have been determined.

Security risk analysis breaks down the risks into two components — the probability or likelihood that a damaging event or condition will occur, and the severity of that 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 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. Human performance should be considered in context of the value of the mitigation measure as part of the risk assessment process.

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

Key points

1. Local liaison is important. Sharing information with partner entities is encouraged. This will achieve a more comprehensive local threat picture than acting alone, reducing duplication of effort and enabling joined-up threat mitigation.
2. Local police may be used as a source of up-to-date local crime information.
3. Share information with your people - encourage and empower them to act on security related concerns and issues that they encounter.

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 to ensure security is given 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 security processes are effective and that the SeMS is fit for purpose.

The governance mechanism should consider matters of strategic security in support of the SeMS 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 data is an honest and accurate reflection of performance;
- 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.

Existing governance structures may be extended to incorporate these governance responsibilities, depending on the size of the Entity and the type and complexity of its operations. For example, some entities maintain a multi-agency Security Executive Group

(SEG)[1] and Risk Advisory Group (RAG)[2], Security Review Board or an equivalent body which could fulfil the governance responsibilities described.

Entities are encouraged to adopt a similar approach where appropriate.

Key points

1. Clear accountability and terms of reference bring dividends.
2. Regular and effective monitoring of performance, with accurate and meaningful data is essential for good governance.
3. Use existing structures where appropriate.
4. A simple diagram can aid communication and understanding of the governance structure.

1 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. For example it may include senior representatives from the airport operator, the local police force, the local police authority and airlines operating at the airport.

2 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.

Chapter 4

Resources

An effective SeMS depends on:

1. **The provision of adequate facilities, resources, 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, services and maintenance**
4. **Effective contracting and oversight of third 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 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;
- emphasising, for appointments to senior roles, the importance the Entity places on security; and
- providing suitably qualified personnel.

Management of Third Party Suppliers

Accountability for any contracted product or service provided by a third party remains with the Entity.

The Entity should define responsibilities within its own organisation for managing contracted security activities, including quality assurance provided by the third party's operation.

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

Receiving Third Party Services

Where the Entity is receiving a third-party service which impacts aviation security, it should, where appropriate, specify in the SeMS any security-related requirements, including the provision of information by the third party, to enable the Entity to assure security performance.

Providing Third Party Services

Where the Entity is providing a security related service to another party, information regarding the assurance of security performance should, where possible, be shared with that party.

Key points

1. Wherever possible, maintain consistent SeMS resource in order to develop expertise and maintain consistency.
2. Senior Managers should lead in the delivery of the SeMS and actively promote a positive Security Culture.
3. Third party providers should be part of the SeMS as well as being managed by it.
4. The heart of a SeMS is the sharing of information and data - delivering a collaborative SeMS.

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 Assessment

The Entity should use performance monitoring and measurement to verify its security performance against the Aviation Security requirements and the Entity's security policy, objectives, identified risks and specified mitigation measures as defined in its SeMS.

This process should include the setting of security performance indicators, as well as security performance targets and measuring the security performance against them. All levels of relevant management should have oversight of key performance indicators.

The performance monitoring and measurement process should include:

- addressing the performance in relation to compliance with the Aviation Security requirements;
- assessing how effective a security process is and not just checking if it is taking place;
- security reviews including trend 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 effectiveness of the management system;
- examination of elements or procedures of a specific operation, such as problem areas or bottlenecks; and
- internal security investigations (including root cause analysis) of security incidents.

Analysis of Data

The Entity should determine, collect and analyse appropriate data to demonstrate the suitability of security processes. The Entity should also 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 causes of poor performance in order to prevent recurrence.

A documented procedure should be established to define requirements for:

- reviewing poor performance;
- determining the root causes of poor performance;
- assessing the role human factors plays as part of the root cause;
- evaluating the need for action to ensure that poor performance does not recur;
- determining and implementing the appropriate action;
- maintaining records of the results of action taken; and
- reviewing corrective action taken.

Preventative Action

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

A documented procedure should be established to:

- identify potential poor performance and the associated cause/s;
- evaluate the need for action to prevent the recurrence of poor performance;
- determine and implement appropriate action;
- record results of action taken; and
- review preventative action taken.

Management of Security Data and Information

. Effective management of security data and information should be protected from interference and access rights should be restricted only to those authorised.

Security Reporting System

The overall purpose of the security reporting system is to use reported information from staff and the public 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 or 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 shared both internally and externally, where appropriate, so that others may learn from them and adapt behaviours accordingly.

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

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, to whom, 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. An Entity's existing "Whistleblower" reporting process may be suitable for this.

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 by those authorised.

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

Quality Assurance of Data and Information

Honest and accurate data is essential for a SeMS to work and for Board and Regulator assurance. 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.

Key points

1. Collection, analysis and sharing of honest and accurate data is an essential SeMS principle.
2. Effective targeted performance measurement and reporting is fundamental to a SeMS.
3. Think wider than security requirements - how can overall performance be improved and potential gaps closed?
4. An open SeMS is a good SeMS. Clear reporting procedures will encourage engagement.

Chapter 6

Incident response

The SeMS should include:

1. **Security incident response processes**
2. **Methods of testing, reviewing and improving the response plan**
3. **A procedure for the introduction of additional security measures**

Incident Response

All SeMS should include response processes for dealing with security incidents. The processes should be exercised and 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 operations 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.

Key points

1. The exercising of security incident response procedures can take many forms and can be of varying scale - the size of Entity largely determines how this is best achieved.
2. Positive SeMS practice is a log of outcomes and improvements subsequently made.

Chapter 7

Management of change

The SeMS should:

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

General Principles

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

The Entity should establish a formal process for the management of change which considers:

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

When business changes are planned the Entity should consider any impact on its SeMS through its security governance processes.

Key points

1. Change from any source can affect security. A robust SeMS will have clear change governance in place to mitigate risk.
2. An internal culture that embraces security will help to minimise unintentional harmful impacts on security.
3. Security needs to have a voice when change is being considered.

Chapter 8

Continuous improvement

The SeMS should:

1. **Seek to improve security performance**
2. **Evaluate all aspects of security provision**
3. **Share security knowledge and skills**

Continuous Improvement

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

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

Similarly, the Entity should seek to improve its SeMS through its security assurance activity which may include:

- internal evaluations;
- independent audits (both internal and external); and
- continuous monitoring of security controls and mitigation actions;
- Initiatives to incorporate considerations around security culture and human factors.

Sharing of Information

The Civil Aviation Authority encourages industry to bring forward ideas that lead to a greater sharing of information in ways that do not compromise the effectiveness of security or disclose sensitive information. In particular, industry is encouraged to collaborate on the development of new security management approaches, techniques and tools to assist in every Entity's continuous improvement.

Key points

1. A critical look at a SeMS by someone not directly involved can bring a fresh perspective and highlight gaps.
2. The sharing of information between SeMS entities will benefit everyone and help build a positive Security Culture.

Chapter 9

Security education

The SeMS should:

1. **Explain how the SeMS principles will be promulgated across all levels of the Entity.**
2. **Tailor the relevance of the security education that is provided to your employees.**
3. **Evaluate your employees'level of security awareness.**

Aims of Security Education

Security education has a key role to play in developing a positive Security Culture.

It may include high-level knowledge of SeMS, knowledge of SeMS concepts and principles, and detailed training in the processes and procedures associated with SeMS. It may also include less formal activity designed to enhance awareness of wider security issues according to the context. It is important to emphasise that the amount and level of detail of security education an individual receives should be proportionate and appropriate to their level of responsibility and involvement in the SeMS.

The Entity should establish an education programme for all personnel within the organisation, including senior management. and should also take into account third party providers and other site users. Entities should consider how to raise awareness for all these groups and should evaluate the effectiveness of the education provided.

Security education should be relevant to each recipient's roles and responsibilities in order to:

- develop and enhance the desired levels of security across the organisation;
- promote security awareness to a wider audience;
- achieve the Security Culture aspirations of the organisation;

Scope of Security Education

The programme should include the following:

A. Operational Personnel

- Security responsibilities, including adherence to all operating and security procedures, recognising and reporting threats;
- Objectives should include familiarity with the Entity's security policy and a clear understanding of their security responsibilities;
- Identify what a positive Security Culture looks like within the organisation and how everyone can contribute to this;
- Contents should include, at a level of detail appropriate to the role:

  a) definition of threats;

  b) consequences and risks;

  c) the SeMS process, including roles and responsibilities; and

  d) the Entity's security reporting systems.

B. Line Managers and Supervisors

- Security responsibilities, including promoting the SeMS, Security Culture and engaging operational personnel in threat and incident reporting;
- In addition to the objectives established for operational personnel, the objectives for managers and supervisors should include knowledge of the security process, threat identification, security risk management, mitigation, and change management;
- In addition to the programme specified for operational personnel, the objectives for supervisors and managers who conduct a security role should also include security data analysis and the importance of data quality assurance.

C. Senior Managers

- Depending on their role this should include, but not be limited to, 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, active promotion of the SeMS Policy and development of a positive Security Culture.

D. SeMS Accountable Manager and Staff at Board Level

- The programme 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, security assurance and development of a positive Security Culture.

Key points

1. A SeMS can only fully deliver when an Entity has a positive Security Culture across the entire business.
2. A Security education programme should reach all stakeholders, and the message be tailored to suit.
3. The sharing of information between SeMS Entities will benefit all and assist in building an industry-wide robust and resilient Security Culture.

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 security communication**

Security Communication

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

Security communication should aim to:

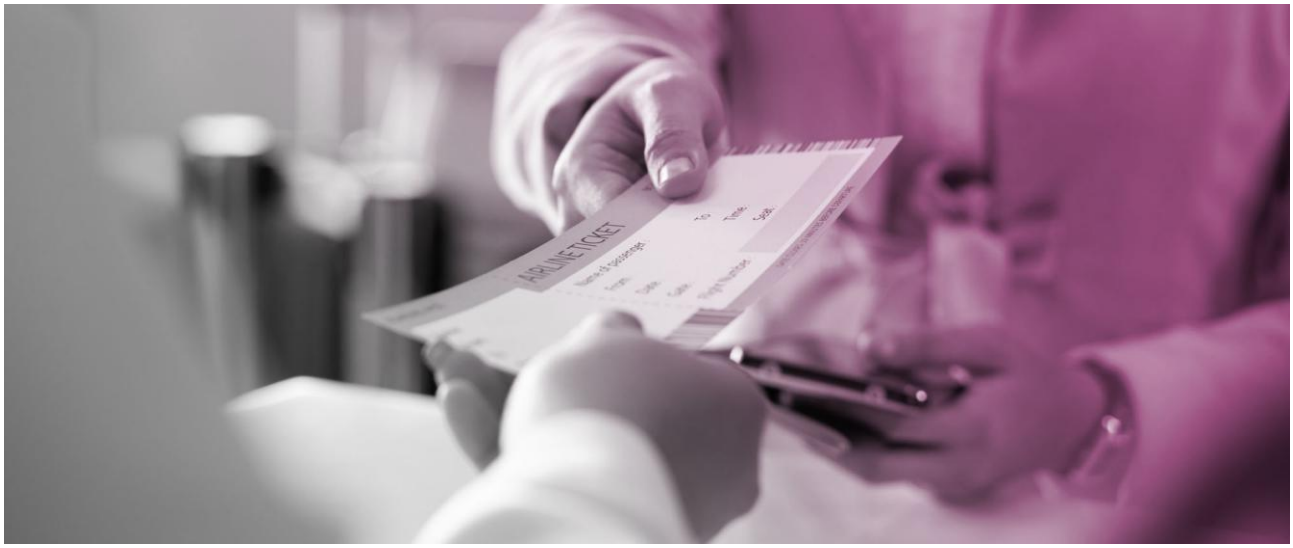
- ensure that personnel are aware of the wider security responsibilities shared by all in the context of the Entity's Security Culture;
- ensure that all relevant personnel are fully aware of the SeMS;
- convey security-critical information;
- explain why particular actions are taken; and
- explain why security procedures are introduced or changed.

Communication Tools

The Entity may use various tools to communicate security information which can be formal or informal means and may include standard operating processes, procedures, briefings, feedback sessions, awareness events or formalised training packages.

Communications should observe protective security markings and dissemination guidance as appropriate.

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



Key points

1. A strong communications strategy will assist you in embedding SeMS and will build upon a positive Security Culture that is integrated across your business.
2. Involving other departments and encouraging contributions to security related communications builds inclusivity in security delivery.

Further information

Cyber Security

"Cyber security is how an individual or an organisation reduces the risk of a cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers) and the services we access – both online and at work – from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on these devices and online."
National Cyber Security Centre – What is cyber security?"

The aviation industry's systems are progressively interconnected, which means an up-to-date awareness of direct and indirect threats to information systems is required.

The CAA oversee a variety of regulations aimed at the protection of an Entity's critical systems and data from unlawful interference, and can also recommend voluntary schemes such as Cyber Essentials from the NCSC.

UK CAA encourages entities to take a dynamic and proactive approach in ensuring the right protection is in place to prevent the occurrence or reoccurrence of a cyber-attack against the Entity.

You should make reference to cyber risk within your SeMS; however, it is understood that for many organisations this may be managed by other individuals or within a different management system. If this is the case, it is important that there is active communication between these systems and that the cyber risk continues to be identified and managed appropriately as a security risk to your organisation within Threat and Risk Management (Chapter 2) of your SeMS.

Visit https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-oversight/ to find more information about CAA oversight of Cyber.