Department for Transport

UK Civil Aviation Authority

Security Management System (SeMS): Guidance for Small Organisations

CAP 1997

Published by the Civil Aviation Authority, 2021

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

First published November 2020
Edition 2 July 2021

Contents

Introduction

Guidance for Small Organisations on Implementing a SeMS

The introduction of Security Management Systems (SeMS) within the aviation sector has been a tremendously positive step, but we recognise that a few smaller organisations have felt anxious about the process, fearing it would be too expensive, too onerous or too complicated to implement. This document aims to address these concerns and provide some initial guidance for any small organisation working within the aviation sector seeking to develop and implement a SeMS.

SeMS is a simple concept:

- It introduces an assurance structure that actively assesses security performance within your operation;
- It uses that performance data to proactively develop corrective actions to reduce risks and safeguard against future events; and
- It develops a management-led, positive Security Culture throughout all levels of your organisation allowing all to recognise the value of strong security performance.

Implementing a SeMS is far simpler than you might think, and most organisations find that many of the components of a SeMS are already in place within their operation. The SeMS Framework is designed to be flexible and can be adapted to suit any organisation, irrespective of size. You can therefore develop an effective SeMS, specifically tailored to suit your operation, and you can start by fully exploiting and developing the systems and processes you already have in place.

There is no mystery to SeMS – an effective SeMS is uncomplicated, easy to understand and straightforward to implement. If you are considering implementing a SeMS, please contact the CAA SeMS Team by emailing SeMS@avsec.caa.co.uk. They will provide guidance on the requirements for your operation and ongoing support as you develop your SeMS. You can also find further information on our website at www.caa.co.uk/SeMS.

Why do we need a SeMS?

To obtain day-to-day assurance that security risks are identified and mitigated effectively, an entity needs an organised, systematic approach and efficient measurement of its security performance. This approach will include both the security measures it takes to meet regulations and those it determines are necessary to tackle any unregulated security risks.

The significance of these unregulated risks should not be under-estimated. While the UK CAA's oversight can provide a "snapshot" view of compliance at a specific time and location, and may draw inferences from it regarding compliance at other times and locations, it does not provide ongoing assurance on a continuous basis. Reliance on compliance with the regulations is simply not enough.

It's true that previously unrecognised threats are constantly evolving - and new threats emerge on a regular basis. Organisations should therefore be constantly alert to the evolving threat picture and be ready to identify new threats, especially threats that the regulations may not yet cover. It is equally important that where they have been identified, these threats and subsequent risks are rigorously assessed, so that adequate, proportionate and achievable mitigations can be put in place.

SeMS will provide for a structured and consistent framework within which you can identify threats, assess and mitigate risks and monitor the effectiveness of those mitigations.

How is a Small Organisation defined?

Safety Management Systems (SMS) classify an organisation as 'small' if the operation employs less than 20 staff. However within SeMS, there is no fixed definition of a small organisation, rather we look at the entity as a whole within the wider context of the sector.

You may consider yourself to be a small entity, either because your employee numbers are low, or you consider yourself to be "small" in comparison to those you see as your industry 'competitors'. However small your organisation may be, the SeMS Framework has been developed alongside industry to ensure it works for every size of entity, whether it has 10 or 10,000 staff. Whatever the size of your business, it is worth remembering your SeMS is tailored to fit your organisation and the environment in which you operate.

Key Components of a SeMS

A SeMS includes the following ten key components, each of which is addressed in some detail by a Chapter of the SeMS Framework:

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

Each key component, or Chapter, is designed to operate in concert with all of the other nine Chapters, and your SeMS will perform at its best when each component is operating effectively alongside the others.

Chapters 1 to 10 of this guide cover each of these components in turn and will explore how they apply to a smaller entity.

Building a Positive Security Culture

One of the most important drivers of a successful SeMS is the work you will do to develop an effective and positive Security Culture. When your employees feel confident and positive about security, and know they are valued and making a difference to the entity's performance by conducting security functions to a high standard, they will appreciate more fully the value of good security performance, rather than viewing it as 'just another job'.

A simple and effective way to communicate the importance of security to your employees is through a focused and structured education programme (chapter 9) which enables them to explore the purpose behind their role and the importance placed upon it by their organisation, as well as the consequences of any decrease in performance standards. This could be delivered through existing communication channels (which are unlikely to incur any additional expense) such as:

- Briefings;
- Recurrent training;
- Staff events; and
- Tool-box talks.

Alternatively, you may choose to introduce a new programme of events to deliver these important messages to your employees, the choice is yours and you are free to utilise whatever methods work best within your organisation.

Positive attitudes towards security can result in a major step forward in raising overall security standards, and ICAO have produced a number of documents which contains helpful suggestions for promoting a positive Security Culture within your business:

https://www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx

The UK CAA have also developed a Security Culture Self-Assessment Tool which may be used to assist you in assessing if a positive security culture exists within your organisation. This can be found at: https://www.caa.co.uk/Commercial-industry/Security/Security-management-systems/Security-culture-self-assessment-tool/

Chapter 1

Management Commitment

SeMS adopts a 'Top-Down' approach, where the Directors and Senior Management Team take an active lead in demonstrating to their employees their commitment to high standards of security performance and promoting the message that security is a priority for their organisation.

Senior managers can signal their commitment by establishing the following:

- Key accountable and responsible person(s) who hold the overall responsibility for the SeMS;
- A clear Security Policy that is actively promoted, and clearly illustrates senior-level commitment to security; and
- A benchmark of clear security objectives and performance standards.

1.1 – Security Accountabilities and Responsibilities

Within the SeMS Framework, two key roles must be established – the 'Accountable Manager' and the 'Security Manager'. These roles can be defined as follows:

- Accountable Manager – The senior person who is ultimately responsible i.e. is accountable for the delivery of security within the entity. An Accountable Manager should be a Director or a senior manager who operates at Board level.
- Security Manager – The subject matter expert whom the Accountable Manager directs to implement and maintain the SeMS, and who utilises the SeMS to provide assurance reports on security performance to the entity. This person would have responsibilities including responding to any security incidents, and may need some training to become fully effective within the SeMS role.

It is good practise to keep the two roles separate where practicable, as this can provide clarity on the specific levels of accountability and responsibility for the SeMS, and will help to make the operation and maintenance of your SeMS more straightforward.

We recognise that this may not be possible for some small organisations because of the small number of people employed, and understand that in some instances it may be necessary for the roles to be undertaken by the same person. If this is the case for your organisation, you can eliminate any confusion or duplication of work by clearly defining all SeMS responsibilities and accountabilities held by the individual, and by documenting which responsibilities are delegated to other employees by them.

1.2 – The Accountable Manager

The Accountable Manager has ultimate ownership of the SeMS and provides leadership, direction and impetus; they are accountable for ensuring that the Security Management System is properly implemented and maintained.

They should have:

- Authority to direct both finance and resource to the security operation;
- Oversight of the key issues of risk management within the entity; and
- Oversight of the entity's assurance programme and its maintenance.

Their technical knowledge and understanding of SeMS should be sufficient to perform this role.

1.3 – The Security Manager

The Security Manager for the SeMS, who may also be referred to as the SeMS Manager, is the focal point for the day to day management and administration of the SeMS, and as such they should have relevant operational experience and a comprehensive knowledge of the systems that support your operation. They should also have an understanding of Aviation Security Management principles, ideally obtained through both formalised aviation security training and practical experience. Please note that your designated Security Manager for SeMS purposes does not necessarily have to hold the job title "Security Manager" within your business.

The employee who is designated as the Security Manager or SeMS Manager in your business position should be responsible for:

- Ensuring that SeMS processes are established, implemented and maintained;
- Promoting security awareness and a positive Security Culture;
- Liaising with local authorities on security-related issues;
- Exchanging valuable lessons learned with other organisations and industry peers;
- Managing internal security incidents and investigations;
- Ensuring identified security risks are managed;
- Maintaining security reporting documentation; and
- Organising security training.

1.4 – Security Policy

Once your two key appointments have been made, the best place to start is your Security Policy. This is a short document, typically consisting of just one page that sets out your security aims and objectives clearly and succinctly. It should be written using plain English so that the information is understandable to your workforce, and it should be communicated to all staff. It can be displayed in prominent parts of the business so that it is obvious and visible - office notice-boards, staff rest areas and Reception areas are ideal places to display your policy. It should also be presented in a way that catches the eye of anyone walking past, so that they will take notice and want to read it!

Your Security Policy is your statement of intent - it explains your organisation's intention and commitment to maintain and improve security standards in all its activities, and is essential in laying the foundations for achieving an effective SeMS and reaping tangible results. You may already have a similar document within your organisation; Aviation Safety and Health and Safety policies are of comparable format, and may be used as the basis for your Security Policy.

The Security Policy should:

- Be signed and endorsed by the Accountable Manager;
- Identify security as a high organisational priority that is mutually supportive of both commercial and operational priorities;
- Reflect organisational commitments regarding security and the entity's proactive and systematic management approach;
- Be communicated throughout the entity;
- Promote a positive and embedded Security Culture; and
- Be periodically reviewed to ensure it remains relevant and appropriate to the entity.
- The Security Policy may include:
- Security reporting procedures, including access to the Anti-Terrorist hotline;
- Include security reporting principles and whistleblowing arrangements; and
- A commitment to:
    - a Continuous Improvement programme;
    - ensure Aviation Security Regulation and all applicable standards are met, and consider best practices;
    - provide appropriate resources; and
    - reinforce security as the responsibility of all personnel.

Chapter 2

Threat and Risk Management

This Chapter focuses on how to identify your entity's current security risks and how to mitigate them. As a small entity, it may be assumed that your risks are lower, and that a person with malicious intent would focus on a larger organisation. In reality, however, smaller organisations are just as likely to be targeted.

A Threat and Risk Management process can be easily established and implemented using three easy steps:

- Identification;
- Assessment; and
- Review.

2.1 – Threat and Risk Identification

Threat and Risk Identification is a vital component of SeMS. Sometimes it is easier to refer to these as 'Security Issues'. Security issues are a form of threat or risk that could cause or create a vulnerability to an attack on part of the aviation sector, whether that be within an airport, an item of cargo, in-flight catering, or from within the aircraft itself. Only when you correctly identify the threats that exist, can you identify the level of risk they pose to your organisation. If you know the level of risk the threats pose, you can proactively manage them by applying risk control measures.

National and international threats are identified and communicated to aviation regulated entities through Government agencies and are mitigated through regulatory measures. Assessing which Aviation Security Regulations apply to your business provides the initial key indicators for where the risks to your business may lie.

An effective SeMS, however, looks outside of these standard parameters, by also considering more local threats. These threats can take into account concerns such as local crime levels, imminent protests, industrial action or any upcoming local events that might increase footfall through or near your premises.

To gain insight into local risks, a larger entity would typically be involved in multi-agency groups where information is shared. This approach to gathering local threat information can be implemented on a smaller scale by organisations like yours.

You may choose to start by building a relationship with your local police force or the local department that you would report any serious security incidents to. These should be listed within your Security Programme. By building a positive relationship with the police, your organisation will receive the latest local criminal and threat information pertinent to your

operation. For smaller airports, or aviation-related businesses located close to an airport, there is guidance on building a more comprehensive multi-agency network on the government website below:

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

A crucial element of a successful SeMS is working in collaboration with as many relevant parties as possible, with the aim of sharing information. Forming a network with local businesses where local security or criminal issues can be communicated quickly and efficiently, can be of great benefit, not only to your entity, but the wider local community. A network such as this, which focuses on security issues, and not commercially sensitive information, should be an attractive prospect for all involved.

2.2 – Threat and Risk Assessment

Once the relevant security issues related to your organisation have been identified, they must be documented and assessed to ascertain:

- The likelihood of an event occurring;
- The potential damage it could cause to the business, and
- What is being done about it, with proposed mitigations.

This does not need to be a lengthy or complicated process and can be documented in a simple risk register.

2.3 – Threat and Risk Review

The contents of the risk register should be reviewed regularly. This review should include:

- Adding any new risks;
- Archiving any obsolete risks;
- Altering any risk mitigation strategies to reflect the likely occurrence of any security risk; and
- Updating who is taking ownership of the risk (if applicable).

The frequency for reviewing the risk register is the choice of your organisation; however, for a small organisation, monthly or even quarterly may suffice.

Chapter 3

Accountability and Responsibilities

When creating your SeMS, levels of Accountability and Responsibilities for the aviation security functions need to be clearly defined, including security governance. In a small organisation, security-related functions may be limited, and the levels of responsibility below the “Security Manager” may be limited to a single supervisor.

Clearly defined roles and responsibilities are essential as they will help the Accountable Manager to put in place a clear security governance structure for the SeMS. This ensures it is operating effectively and providing maximum benefit to your organisation.

In order to support the Accountable Manager effectively, the governance structure should:

- Monitor security performance against your organisation’s Security Policy and objectives;
- Monitor the effectiveness of your organisation’s operational security and aviation security management processes;
- Ensure that the reported data is an honest and accurate reflection of performance;
- Ensure that any corrective actions are taken in a timely manner; and
- Ensure that appropriate resources are allocated to achieve the organisation’s intended security performance objectives.

If, as part of your SeMS, you work in collaboration with any other entities, you may expand security governance set-ups to incorporate these companies.

Chapter 4

Resources

For your SeMS to work effectively, it needs adequate resourcing, but this doesn't have to mean an increase in headcount. A SeMS ensures that sufficient resource (whether it be employees or equipment) is allocated to a particular task, and that the resource is deployed as efficiently as possible.

When allocating resources to a task, you should determine the following:

- The number of personnel required for the task;
- The required competencies and level of aviation security training; and
- The importance that your organisation places on security and the promotion of this by those in senior roles.

All personnel within your organisation that will be directly contributing to security processes should be competent to undertake their roles and have appropriate training, skills and experience.

There may be some occasions where it is determined that a task may require additional resource, whether that be staff or equipment. In these cases, the expectation would be that the Accountable Manager and Security Manager agree on the scale of the additional resource that is required and the Accountable Manager will act to ensure that relevant resource is directed to the where it is needed. Small organisations tend to hire new staff or purchase new equipment less frequently than larger organisations, however a smaller organisation may be more agile and better able to respond quickly to such a requirement.

An effective SeMS will enable you to provide clear evidence to determine whether the additional resource is required, or not, and the subsequent benefits may be evident even before presenting a business case.

4.1 – Management of Third Party Suppliers

Under current regulations, the ultimate responsibility for any product or service that is provided by a designated third party remains with your organisation. While utilised less frequently in small organisations, third party providers may provide services such as x-ray screening, manned guarding and transportation.

If this is relevant to your organisation, it is imperative to define within your SeMS:

- The standard of security performance that is expected;
- The responsibilities of the third party provider with regards to reporting, Quality Assurance etc.; and

- A Quality Assurance plan to ensure the third party is providing the service your organisation has contracted for.

As a small organisation, you may find it easier to maintain regular, open and honest dialogue with your third party providers about their performance, supported by relevant assurance data. It is worth bearing in mind that third-party employees should be able to demonstrate the same levels of competence and training that you would expect from your own staff.

Ongoing dialogue with your third party provider is essential, not only for maintaining effective oversight of their performance, but also for providing a channel through which you can promote security as a shared responsibility, as well as other key messages that can help to embed a positive Security Culture.

Chapter 5

Performance Monitoring, Assessment and Reporting

Experience tells us that this Chapter of the SeMS Framework is most likely to cause reluctance to pursue SeMS for a small entity. However, concerns that this Chapter requires endless amounts of paperwork and reports, are simply not founded.

Aviation Security Regulation requires entities to undertake Quality Assurance of their aviation security operations. A SeMS will help to provide structure to this QA activity, so that performance monitoring processes are more straightforward, and the information obtained is relevant and easier to understand. This Chapter addresses the gathering of data and how to use it to improve security performance standards.

5.1 - Performance Monitoring and Measuring

Your organisation should use performance monitoring and an appropriate measuring tool to verify the performance of its security processes, and you may use the relevant aviation security requirements, your Security Policy, your organisation's security objectives, identified security risks and any specified mitigation measures as defined within your SeMS as a baseline.

This process should include the setting of appropriate security performance indicators and targets to measure against, and senior managers should have oversight of those security performance indicators, and assurance that the required standards have been achieved.

Your performance monitoring and measurement processes should include:

- Addressing performance in relation to compliance with Aviation Security Regulation;
- Assessment of how effective the security processes are and not just that they are in place;
- Security reviews including a review of any trends, to be conducted during the introduction and deployment of new technologies, change or implementation of procedures, in situations of structural change, and to investigate an increase in security incident reports;
- Security audits which focus on the effectiveness of the management system;
- Examination of any problematic areas of the business, or a specific area of compliance the organisation is struggling to meet; and
- Internal security investigations of security incidents.

These processes form the cornerstone of your SeMS, and the other Framework Chapters work closely in conjunction with them. This Chapter encourages your organisation to provide a clear structure to many functions you that may already be undertaking.

5.2 - Analysis of Data

You may already collate data as part of your internal audits, but if any of it does not provide an insight into your organisation's security performance, you should consider whether it is worth continuing to collect it. As part of Continuous Improvement, you may find you can simplify your internal audit process and stop gathering meaningless data.

As a small organisation with limited resources, eliminating unnecessary work could bring you significant benefits.

5.3 - Corrective and Preventative Action

After analysing your data, you will wish to take action to either correct areas of poor security performance (corrective action), or put in place processes aimed at preventing potential causes of poor security performance (preventative action).

A documented process should be established, in order to:

- Review areas of poor performance;
- Determine causes of actual or potential poor performance;
- Evaluate the actions required to ensure that an area of poor performance doesn't occur again;
- Record the actions that have been taken; and
- Review any corrective and preventative actions taken.

It is worth noting that it is not necessary to use an IT system to document this activity. A smaller organisation may find that a paper-based approach is a cheaper and more accessible option that can still achieve the desired outcomes.

5.4 - Security Reporting System

A Security Reporting System is a function for collating reported security information from your employees and is used to improve your organisation's security performance. A Security Reporting System, when working correctly, should promote inclusivity and make employees feel valued as they see that the information that they are reporting is acknowledged and acted upon by managers.

A Security Reporting System should never be used to attribute blame to groups or individuals as this can stifle the development of a blossoming Security Culture, and is likely to have a negative impact on security performance across the organisation.

Your reporting process should be simple and clearly defined, and should include details as to what, how, where, to whom and when to report.

The objectives of the Security Reporting System are to:

- Enable an assessment of the security implications of each relevant occurrence or serious incident, including previous similar events, so that appropriate action can be initiated; and
- Ensure the knowledge of relevant occurrences and serious incidents is shared both internally and externally, where applicable, so that others learn from them and adapt processes accordingly.

A Security Reporting System should include a feedback system to the reporting person on the outcome of an occurrence, either in writing or verbally from the Security Manager. It is recognised that an online system could prove to be challenging to introduce within a small organisation, and cheaper and simpler alternatives may be used which can be equally effective.

The underlying principle is that the reporting system must allow an individual to report anonymously and in confidence. This can be achieved in a number of ways, including using an anonymous suggestions or feedback box, and using an external company to provide an anonymous email or telephone service.

5.5 - Management of Security Data and Record-Keeping

All relevant security data should be recorded and held securely so that it is only accessible to appropriate members of staff. If all staff have access to the same online systems, a defined area where files can be kept securely, or a password-protected area online would be the most suitable way of storing this information.

Chapter 6
Incident Response

A SeMS will require effective incident reporting processes to be in place for dealing with security incidents, whether it's a minor incident dealt with internally, or a major event which require the intervention of law enforcement. This is a reactive form of security management, but one that can also facilitate Continuous Improvement.

For a small organisation, a security incident or error may happen only very rarely, however, lessons can still be learnt and incidents can be prevented from happening again. How your organisation prepares to deal with any potential incidents can be a sign of organisational strength, and results in less of a negative impact should an incident occur.

When an incident occurs it is essential that it is documented, so that lessons can be learned from the event. This task can be split across the individual/s who report the incident, and the Security Manager, who takes ownership of the rectification plan and updates any incident response plans already in place. This collaborative approach to learning from an incident can help employees feel a valued part of the security team and will further assist in building a positive Security Culture.

Any new incident response plans or mitigation strategies that are brought into effect following an incident is likely be easier to communicate within a small organisation as the messages need to be cascaded to fewer people. Despite this, it is always essential to have effective communication channels in place as part of a healthy, functioning SeMS (see Chapter 10 for further information on Communication).

Chapter 7
Management of Change

Change within an organisation can significantly disrupt the security function, even if there was no intention to do so. Change may introduce new risks or have a profound effect on the risk mitigation strategies the organisation already has in place.

Changes that are relevant to a smaller organisation could be obvious; an increase in business resulting in current resources being overstretched, or less obvious, such as internal building work altering evacuation plans. Whenever change within the organisation takes place, it is imperative that the security function is consulted so that the entity can capture, assess and mitigate against any potential risks and a SeMS will support the introduction of a formalised Change Management process. As a smaller organisation, you may find it easier to manage change, as consultation and decision making is likely to be shared across a smaller number of individuals. You may well find that a very simple change management process can work extremely effectively, where all areas / individuals are consulted at the start of any change process.

Chapter 8

Continuous Improvement

All businesses, large or small, continuously seek to innovate, increase efficiency and improve standards and the security sector is no different. Under this Chapter of the SeMS Framework, an organisation should be continuously looking to analyse the information it receives about its security performance from proactive or reactive evaluations of current processes. Ideally, the following areas should be under regular review:

- The organisation's Security Policy and procedures;
- Any relevant facilities, security equipment and documentation;
- The effectiveness of the internal Quality Assurance regime;
- Employee security performance against the organisation's set security objectives and performance goals; and
- The organisation's processes for recording, assessing and mitigating against any security incidents.

How often these reviews are undertaken can be determined internally, factoring in such variables as seasonal influxes and unforeseen incidents. The advantage for smaller organisations utilising a robust Continuous Improvement plan is that any resulting change is typically easier to introduce, and avoids the complexities encountered by large multi-site operations.

Chapter 9

Security Education

All employees need to understand the purpose of their role and their responsibilities with regard to both security and the SeMS, and establishing a structured education programme for all levels of staff, across all departments within the business will ensure that they have the relevant knowledge and skills to perform their role to the required standard. This may be covered through formal or informal training, or by other simple means such as requiring staff to read and confirm their understanding of the SeMS Manual.

SeMS education should include:

- Security Culture;
- Security Assurance;
- Security Promotion;
- Security roles and responsibilities; and
- Establishing acceptable levels of security.

There is no requirement for additional training to take place, however, and SeMS can be built into any form of recurrent aviation security training or education you currently undertake, without adding to your overall expenditure. As with all Chapters of the SeMS Framework, no Chapter should impede your organisation from reaping the benefits that SeMS will bring.

9.1 – SeMS Education

All forms of SeMS training and education must be adapted to individual job roles and the SeMS Framework document explains which level of SeMS education each should achieve. Please note, it is not mandatory to have all of these roles within your organisation and some may overlap due to the smaller number of employees:

A. Operational Personnel

- Security responsibilities, including adherence to all operating and security procedures, and recognising and reporting threats;
- Familiarity with the Security Policy and ensure understanding of the entity's SeMS;
- How everyone can contribute to a positive Security Culture, 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) Security reporting and the Security Reporting System.

B. Managers and Supervisors (in addition to Operational Personnel objectives)

- Security responsibilities, including promoting the SeMS and Security Culture, and engaging operational personnel in threat and incident reporting;
- Detailed knowledge of security processes, threat identification, security risk management and mitigation, and Change Management; and
- Security data analysis and the importance of data Quality Assurance.

C. Senior Managers

- Security responsibilities in relation to Aviation Security Regulation, the entity's security requirements, allocation of resources, ensuring effective internal security communication, the active promotion of the SeMS Policy, and development of a positive Security Culture.

D. Accountable Manager

- 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.

Depending on the nature of your business, you should consider extending your education programme more widely to include people other than those working in a security related role such as:

- Other departments within your business e.g. HR or Finance;
- Third party service providers; and
- Other members of your wider community, including other organisations utilising your site or passengers.

Your education programme may be formal or informal, depending on the intended audience, and although it doesn't need to be expensive or complicated, it should be relevant and meaningful for them.

You may wish to consider working in collaboration with other organisations, such as local police or an airport who can assist with promoting key messages about the shared responsibility for security across your operation.

Chapter 10
Communication

Effective communication is a vital component of a successful SeMS and this Chapter of the SeMS Framework is intended to ensure that an organisation, regardless of its size, considers how best to communicate with its people, so that all security messages are relevant, easily understood by the intended audience and conveyed to staff in the quickest and most effective way possible. This will include communicating your SeMS objectives and procedures to all relevant persons and partner organisations, to further reinforce the importance of security to the entity.

An effective communication plan should:

- Ensure all personnel are aware of the wider security responsibilities shared by all to aid in building a strong Security Culture;
- Ensure all relevant personnel are fully aware of the SeMS;
- Convey security-critical information; and
- Explain why particular processes or actions are being taken, to promote inclusivity of the security process.

As a small organisation you may assume that this will be a quick and simple task, since your communications need to reach fewer people. That may well be true however, for you to be sure that your communications are effective you will require assurance that the security messages have not only been received, but that they have also been understood.

The easiest way to achieve effective communication is to convey messages through a variety of means. You may already be utilising some or all of the following examples:

- The SeMS Manual;
- Security-related posters;
- Email updates;
- Team meetings and /or Morning briefings; and
- Security newsletters, notices and bulletins on staff notice boards.

It is also worth asking local police or other relevant industry bodies if they have posters, leaflets or are able to provide guest speakers as a means of promulgating messages to your staff.

You can assess the effectiveness of your security communications in a variety of simple ways that will not incur any additional cost:

- “Walking the floor” and talking with staff directly to ensure that the security information has been understood;
- Observing whether a new procedure is being correctly adhered to; and
- Use a briefing session or email communication to invite feedback or questions on a specific security related topic.

Understanding which means of communication are most effective in delivering information to your operation means you will be in a stronger position to optimise your future communication strategies.

Implementing a SeMS

Developing and implementing a SeMS should be undertaken at a pace that suits your organisation. There is no fixed time-frame in which to complete the process once your SeMS journey has begun, although you will wish to maintain momentum in implementing your SeMS, as this will enable you to capitalise on the time and effort you invested its implementation, and exploit the advantages it delivers, with our full support.

The development of a SeMS is split into 4 manageable phases.

Gap Analysis

Your starting point must be to have a solid understanding of your entity's current processes and systems, and completing a Gap Analysis is your first step towards implementing a SeMS. The Gap Analysis allows you to review the processes you already have in place, and identify any areas where improvements or amendments need to be made to bring them in line with the standards outlined in the SeMS Framework document.

This process is crucial in ensuring that senior managers are fully sighted when committing to implementing a SeMS, and indeed many entities have shared with us that they have found completing this document extremely helpful to them in identifying areas of vulnerability where they had previously assumed their processes were robust.

To download a copy of the Gap Analysis form, please visit www.caa.co.uk/sems.

Phase 1 Assessment – SeMS is Present and Suitable

When the entity is ready, the CAA will conduct a Phase 1 Assessment to determine whether the SeMS is "Present and Suitable". Evidence will be required to demonstrate that appropriate and documented processes and governance are in place, or will be implemented in due course.

A meeting will also be held between the Accountable Manager and a CAA manager to determine whether the Accountable Manager has been appropriately appointed, understands the purpose of the SeMS and can demonstrate their commitment not only to the process, but to the ongoing maintenance of the SeMS itself.

Phase 2 Assessment – SeMS is Operating and Effective

Following a successful Phase 1 Assessment, the entity will continue its SeMS development into Phase 2, progressing the SeMS to the point where it is "Operating and Effective". At this point the SeMS is functioning and is utilised to manage security and build a body of evidence of performance data and governance records.

Throughout Phase 2, CAA regulatory compliance oversight of the entity will continue as before. In parallel, the Lead Auditor will liaise with the entity to ensure that it builds up the body of evidence that it will need to meet the required standards of a Phase 2 Assessment.

Once the entity has built up evidence that the SeMS is Operating and Effective, normally after a period of 6 months or so, the CAA will conduct a Phase 2 Assessment. This assessment reviews the SeMS in more depth and will determine if the entity is effectively managing security through the documented, formal processes set out in Phase 1, and producing and using the relevant outputs.

As part of this, senior CAA managers will conduct a formal interview with the Accountable Manager. Where the entity's SeMS is determined to be both operating and effective, it will be designated as a Phase 2 entity and certification will be awarded in person by a senior CAA manager.

Phase 2B – Continuing Assurance

Following a successful Phase 2 Assessment, the entity will move into Phase 2B - Continuing Assurance. In this phase, the designated Phase 2 entity is required to provide ongoing assurance that their SeMS continues to operate effectively. To this end, the entity submits quarterly SeMS Performance Data to evidence that the SeMS is actively utilised to manage security performance.

In addition to this, an entity is subject to a Phase 2B Assurance Assessment and operational Assessment in order to maintain its Phase 2 status.

Guidance and Support from the CAA

Throughout the whole of the SeMS development process, you will be supported by your Lead Auditor and the SeMS Team. They will be your point of contact for any queries or concerns, and will provide one to one guidance and support.

If your organisation is considering implementing a SeMS, or you have any queries, please contact your Lead Auditor, or any member of the SeMS Team at SeMS@avsec.caa.co.uk. We will be delighted to help you.

Further Reading

The following information is available online at www.caa.co.uk/sems:

CAP 1223: Framework for an Aviation Security SeMS

- The official SeMS Framework document that is applicable to all aviation security entities, this document provides details of the standards to be met in each of the ten Chapters.

CAP 1224: A Guidance Note for Accountable Managers

- This provides a concise overview to Accountable Managers of the purpose and advantages of implementing a SeMS, and the role of the Accountable Manager.

CAP 1273: Implementing a Security Management System: An Outline

- This guidance document provides information about how to introduce a SeMS Framework and its underlying principles to your organisation.

CAP 1297: Security Management Systems (SeMS): Frequently Asked Questions

This useful FAQ document should answer any questions you might have about developing a SeMS within your organisation. If there are any questions left unanswered after reading this, please do get in touch with the CAA SeMS Team at SeMS@avsec.caa.co.uk.

Gap Analysis and Assessment Record

- This document is used by both an entity and the CAA as a record of the assessments conducted at each phase of SeMS development up to and including a Phase 2 Assessment. It includes the Gap Analysis form which you can use to determine which components of the SeMS Framework your organisation already has in place - you'll be surprised how much you are already doing! After completion, please contact your Lead Auditor or the CAA SeMS Team at SeMS@avsec.caa.co.uk for further guidance on the next steps to take.

Industry Best Practice

- Upon developing your SeMS, we will share best practice that we have seen from industry and put you in touch with industry partners who will happily share with you processes and ways of working that they have found have assisted them.