



Department
for Transport



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

You can copy and use this text but please ensure you always use the most up to date version and use it in context so as not to be misleading, and credit the CAA.

First published November 2020
Edition 2 July 2021

Contents

Introduction	5
Guidance for Small Organisations on Implementing a SeMS	5
Why do we need a SeMS?	5
How is a Small Organisation defined?	6
Key Components of a SeMS	6
Building a Positive Security Culture	7
Chapter 1 - Management Commitment	9
1.1 – Security Accountabilities and Responsibilities	9
1.2 – The Accountable Manager	10
1.3 – The Security Manager	10
1.4 – Security Policy	11
Chapter 2 - Threat and Risk Management	12
2.1 – Threat and Risk Identification	12
2.2 – Threat and Risk Assessment	13
2.3 – Threat and Risk Review	13
Chapter 3 - Accountability and Responsibilities	14
Chapter 4 - Resources	15
4.1 – Management of Third Party Suppliers	15
Chapter 5 - Performance Monitoring, Assessment and Reporting	17
5.1 - Performance Monitoring and Measuring	17
5.2 - Analysis of Data	18
5.3 - Corrective and Preventive Action	18
5.4 - Security Reporting System	18
5.5 - Management of Security Data and Record-Keeping	19

Chapter 6 - Incident Response	20
Chapter 7 - Management of Change	21
Chapter 8 - Continuous Improvement	22
Chapter 9 - Security Education	23
Chapter 10 - Communication	25
Implementing a SeMS	27
Gap Analysis	27
Phase 1 Assessment – SeMS is Present and Suitable	27
Phase 2 Assessment – SeMS is Operating and Effective	27
Phase 2B – Continuing Assurance	28
Guidance and Support from the CAA	28
Further Reading	29

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.