UK
Civil Aviation
Authority

Security Management Systems (SeMS) Frequently Asked Questions

CAP 1297

Industry FAQs Contents

Background to SeMS

Why do we need SeMS?

In order to have day-to-day assurance that all security risks are being identified and mitigated effectively, an entity needs an organised, systematic approach and effective measurement of its security performance. This should include both the security measures it takes in response to regulations and those that it has determined are necessary to tackle any unregulated security risks.

The importance of this second group of risks should not be underestimated. Reliance on compliance with the regulations is not enough and previously unrecognised threats emerge on a regular basis.

CAA oversight alone cannot and should not assure continuous compliance – it can only verify compliance at a specific place at a specific time and draw inferences from that.

Therefore, organisations should always be alert and poised to identify new threats, especially those threats that the regulations do not cover or threats that occur as a result of the implementation of specific regulations. Equally important is, having identified these threats and consequent risks, that an entity conducts a rigorous assessment to ensure that adequate, proportionate and achievable mitigations are implemented accordingly.

SeMS provides a structured and effective way to identify and mitigate risks, and provide assurance at all levels.

What is the SeMS Framework?

The SeMS Framework can be regarded as the high-level specification for an effective SeMS. It describes the ten key components of a SeMS, and the principles behind them, but does not dictate how an organisation must implement them. This means that the Framework is flexible and straightforward to apply within an organisation.

Alongside the SeMS Framework (CAP 1223)[1] and Guidance for Accountable Managers (CAP 1224)[2], the CAA has also published “Implementing SeMS: An Outline” (CAP1273)[3] to provide guidance on implementing a SeMS. This summarises the key points with regards to the Framework, the CAA’s approach to an industry-wide roll-out of SeMS, and how SeMS implementation may be managed. Our CAP publication on “Guidance for Small Organisations” provides tips and further guidance for implementing a SeMS, within their specific context.

[1] http://www.caa.co.uk/CAP1223

[2] http://www.caa.co.uk/CAP1224

[3] http://www.caa.co.uk/CAP1273

We have a mature and integrated Risk Management system already. Why do we need to sign up to SeMS? Are there advantages to beginning to implement this now?

Experience in implementing the CAA's SeMS Framework has demonstrated the following advantages:

- It creates Board Level accountability for security, and enables them to monitor compliance with AvSec requirements as well as meeting QA requirements under current regulation;
- It drives a more assurance based regime;
- It encourages transparent and verifiable security;
- It enables more effective use of existing tools and systems;
- It supports threat assessment methodology; and
- It empowers and promotes Security Culture and pro-active reporting.

By starting SeMS now, an entity can share expertise and best practice to the benefit of all.

Is SeMS compulsory?

SeMS is not mandatory at the time of writing. However, the UK CAA supports a proposal to make SeMS a regulatory requirement and we are working with the DfT who are actively considering this.

Is SeMS suitable for IFS and Cargo?

The SeMS Framework is designed to fit all sectors and the development was guided by a working group representing all four sectors of industry, namely Cargo, IFS, Air Carriers and Airports. Entities of all sizes from all sectors are now actively implementing a SeMS and may find it helpful to read our CAP document "Guidance for Small Organisations", which includes some useful guidance for smaller entities.

Is a SeMS useful – and achievable – for a small organisation?

The SeMS Framework is designed to be adaptable to fit all sizes and types of organisation(s). An organisation should therefore determine for itself the degree of detail and record keeping required to achieve its aims, based on its SeMS needs. For example, in a very small organisation the Accountable Manager may also be the owner of the business and/or responsible for the delivery of security within the entity. In such cases communication, culture change, and performance measurement may be simpler than it is for large organisations.

Both large and small entities have already successfully implemented a SeMS and its value is proven. See our CAP document "Guidance for Small Organisations", which includes some useful guidance for smaller entities wishing to implement a SeMS.

Implementing a SeMS

Who should I speak to if I am considering implementing a SeMS?

If you are a directed party you should talk to your Lead Auditor in the first instance. You may also contact the SeMS Team directly at sems@avsec.caa.co.uk.

How do we go about implementing a SeMS?

We recommend that you treat the implementation of your SeMS as part of your business. You should start by completing a Gap Analysis, which is your first essential step in identifying any processes and procedures that require additional work to meet the requirements of the SeMS Framework. This information enables you to finalise or re-validate senior management commitment before you draw up your implementation plan. For more detail on how to implement a SeMS, see CAP 1273 “Implementing a Security Management System: An Outline”.

Is it expensive to develop a SeMS?

Developing a SeMS does not necessarily have to be a costly exercise and does not require sophisticated electronic systems. We encourage you to utilise and optimise existing processes and systems wherever possible, as appropriate for your organisation.

Gap Analysis

How much detail do I need to include in my Gap Analysis?

Your responses to the questions in the Gap Analysis do not need to be lengthy or overly detailed. The purpose of the Gap Analysis is for you to be able to identify, at the start of the SeMS process, those areas where you believe you have a suitable process already in place, those areas where there is currently no process in place, or where the process requires some improvement to bring it into line with the standards set out in the Framework document. This is crucial information as it enables an organisation to be identify areas requiring development and allocate appropriate resources to develop these.

The Gap Analysis document can be found at https://www.caa.co.uk/SeMS.

Implementing a SeMS – Phase 1

How do I prepare for a Phase 1 Assessment?

The purpose of a Phase 1 Assessment is to establish if your SeMS is “Present and Suitable”, so your organisation should ensure that you are able to clearly describe or demonstrate how you plan to meet the requirements of the SeMS Framework prior to a Phase 1 Assessment.

A Phase 1 Assessment focuses on understanding whether the proposed approach is appropriate and meets the standards as set out in the ten Chapters of the Framework.

When preparing for Phase 1 Assessment, you may wish to:

- Conduct a final sense check across all Chapters of the Framework to ensure that your SeMS is ready for a Phase 1 Assessment;
- Speak with your CAA Auditor about any specific areas of concern;
- Be sure that the person or persons undertaking the assessment with the CAA understands your proposed ways of working with regards to governance, Risk Management, internal Quality Assurance, management of third parties, management of change, training, communications and Security Culture;
- Check that the person(s) present have access to, and are comfortable with, using any systems or platforms you wish to use to demonstrate your intended processes;
- Be sure to have relevant documentation available in order to evidence the process that you plan to use, if your system is paper based; and
- You may wish to refer to the CAA Guidance for Evidence document for the Phase 1 Assessment, which provides examples of the type of documentation that we are likely to require.

The Phase 1 Assessment is focused purely on understanding whether the SeMS appears appropriate, and suitable. As such you are not required to present evidence that it is already in operation, however, you should have credible plans in place to demonstrate that your organisation’s SeMS will meet the requirements of the SeMS Framework in due course.

Who should be present for a Phase 1 Assessment?

The person who manages the SeMS, such as your Security Manager or SeMS Manager, is the person who will be best placed to facilitate the assessment.

You may wish to invite other colleagues to attend for all or part of the assessment as they may be more able to describe or demonstrate in some detail how a specific process or system(s) is intended to work.

The Accountable Manager is not required to be present for the assessment itself, but will be required to attend the Phase 1 Accountable Manager meeting held after the Phase 1 Assessment is completed, for which a suitable date and time will be agreed.

How long will the Phase 1 Assessment take?

The length of the Phase 1 Assessment will vary according to the nature of your organisation.

Smaller organisations will find that the assessment is likely to be easily completed in a single day. Larger organisations may find that two or more days are required to complete the assessment, depending on the size and nature of the organisation.

Is there any benefit in combining Safety and Security Risk Registers, or Safety and Security policies?

You may combine your Safety and Security Risk Register or your Safety and Security policies if you wish, as long as the appropriate security elements are clearly identified, actioned and evidenced. The entity must ensure however, that only an appropriately trained and experienced person within the organisation reviews, analyses and actions the security elements of a document when both the safety and security elements have been included.

My organisation is committed to educating all our staff (not just security staff) about security, but our current budget is extremely limited. Do you have any cost-effective suggestions for ways of educating our people?

Security education does not need to be costly and there plenty of free sources of information and training available. The GOV.UK website has some useful links and information:

- ACT app - this is a free app that is run by Counter Terrorism Policing which may be beneficial for Security Managers / Site Security Representatives. It allows users to access the latest protective security advice 24/7. Available from Google Play or App Store.

- There are Counter Terrorism Security Advisors (CTSAs) at each local police force who can visit a business and provide useful information. Details of this can be found here: https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers.

- You can ask the CTSAs about SCaN workshops and they may be able to arrange modules specific to the different people you have within your organisation. Details of this can be found here: https://www.gov.uk/government/news/security-training-package-empowers-staff-to-see-check-and-notify-scan.

- https://ct.highfieldelearning.com/. This is a free “Action Counters Terrorism” awareness online training session that you can sign up to as an organisation. It takes 45minutes to complete and explains how to spot the signs of suspicious behaviour and how to help yourself, others and emergency responders in the event of an attack. It is very generic and focuses specifically on terrorism, but it covers basic responsibilities and could be appropriate for third party staff working at an airport, for example.

- You should also consider liaising with your local police - they may be able to attend your site and provide some relevant information or updates to your staff. This could be particularly useful for smaller cargo or IFS organisations.

- CPNI – CPNI provide free information and guidance on a range of relevant topics including IT security “Think before You Link” and Insider Threat.

- The CAA – representatives from the CAA would be more than happy to visit your site to discuss their role and responsibilities. They can tailor this to a specific area (for example Covert Testing) or can discuss SeMS, compliance or the work done by the CAA, DfT and UK Government in overseeing Aviation Security. If you are interested in this then please talk to your Lead Auditor or a member of the SeMS Team.

Implementing a SeMS – Phase 2

How do I prepare for a Phase 2 Assessment?

At the Phase 2 Assessment you will be asked to evidence the processes described within your Phase 1 Assessment, and provide assurance that the SeMS is "Operating and Effective". See our "Industry Guidance for Evidence - SeMS Phase 2 Assessment" document for examples of the types of evidence we will need to see.

Check that all staff providing the required evidence will have access to the records and systems on the day of the assessment: where there are a significant number of people involved, discuss with your CAA Auditor how you would like to handle this.

Identify in advance the key personnel who need to be present during the assessment and confirm they are available

If you anticipate any specific issues ahead of the assessment, please contact your CAA Auditor to discuss how these can be managed.

Who should be present during a Phase 2 Assessment?

The Phase 2 Assessment is likely to be facilitated by the Security Manager (also known as the SeMS Manager in some organisations), as they are likely to have in depth knowledge of the SeMS itself and be able to access the data required. For very large entities, it may be that the evidence required is accessed through several different individuals, and the entity should ensure that they are available as required.

We do not require the Accountable Manager to be present for the Phase 2 Assessment, although they are very welcome to attend if they wish. However they will be required to take part in a Phase 2 Accountable Manager interview after the Phase 2 Assessment has been completed, this will be conducted on a mutually convenient date.

What format should the evidence be in? Must it be electronic or is paper OK?

We do not stipulate what form the evidence should take. Electronic evidence is preferred, but if your systems are paper-based, this is equally acceptable.

How long will a Phase 2 Assessment take?

This very much depends on the size and nature of your organisation. We would expect to complete an assessment for a small organisation with just one site in a single day. We would expect the assessment for a very large entity, or one with multiple and varied sites, to take two or more days to complete.

Implementing a SeMS – Phase 2B

Do I have to submit the quarterly SeMS Performance Data (SPD) reports to you?

Yes, as part of the CAA's continued assurance that an entity's SeMS remains Operating and Effective, and, as a precursor to Risk Based Oversight (RBO), entities will need to submit quarterly SPD reports to the CAA. The quarterly submission of SPD data is a key element in maintaining your Phase 2 status.

When do I need to submit the SPD to the CAA?

Reports should be submitted the week leading up to and including the first day of January, April, July and October each year. If you know in advance this will not be possible, you should contact the SeMS Team to inform them and agree alternative arrangements. Further details on this, and the processes adopted by the CAA if submissions are not received, can be found within the SeMS Phase 2B guidance documentation, which is available to entities on reaching Phase 2B.

Is the Phase 2B Assurance Assessment a requirement for Phase 2B?

For the CAA to maintain assurance of an entity's SeMS an Assurance Assessment will be required in addition to the quarterly SPD submissions. This assessment will be preannounced and arranged with you to ensure the dates are suitable for both parties.

Do I need to prepare anything for the Phase 2B Assurance Assessment?

During the assessment, the CAA Auditor will ask a series of questions about how you meet the standard set out in the Chapters of the SeMS Framework and will record your responses in an Assurance Assessment report. Your responses will need to be supported by documented evidence.

It is recommended that you prepare for the assessment by familiarising yourself with the format of the Assurance Assessment report. This can be obtained from your Lead Auditor. You should also consider how you will evidence your SeMS, as well as how you will access your policies and procedures, your QA findings and any subsequent action you have taken to address areas that have required further attention. Electronic access to these is preferable to printed copies.

My organisation has several sites in the UK. Will the CAA conduct an Assurance Assessment at each site?

The CAA will conduct the Assurance Assessment at only one of your sites. However, we will also need to conduct Operational Assessments (to gauge employees' understanding of security and their security responsibilities) at a selection of your other sites in the UK. Further details on this will be provided to an entity when they reach Phase 2B.

My organisation has many sites – which sites will you visit when you conduct Operational Assessments?

The CAA will conduct Operational Assessments at all regulated sites on a rotational basis. We will ensure we visit all sites at least once every 5 years, with an emphasis placed on larger sites or those identified as higher risk. Further details on this will be provided to an entity when they reach Phase 2B.

Now I am submitting SPD reports on a quarterly basis, will this change the CAA's compliance oversight regime for my organisation?

This is our vision, and a strategic goal of the CAA. Having assurance of an entity's security operation is the first step in our move towards a Risk Based Oversight, however, this will require further development. This work has now started, and we intend to work alongside industry colleagues to progress this.

If my organisation loses its status as a designated Phase 2 entity, how can I regain it?

This will be considered on a case by case basis and discussed with the entity, as the process for regaining Phase 2 status will be dependent on the outcome of the last Assurance Assessment and the amount of time that has elapsed since it was conducted. It may involve conducting a further Assurance Assessment on site, or possibly a full Phase 2 Assessment. Further details on this will be provided to an entity when they reach Phase 2B.

Who can I contact if I need additional guidance or support with SPD submissions or the Assurance Assessment?

Your Lead Auditor and the SeMS Team are available to offer support and guidance on completing SPD reports or preparing for an Assurance Assessment. Contact your Lead Auditor directly or email the SeMS Team at SeMS@avsec.caa.co.uk.

My organisation has appointed a new Accountable Manager. Do we need to inform the CAA?

If the designated Accountable Manager within a SeMS entity changes, it is important that the newly nominated Accountable Manager is fully briefed and skilled on SeMS and their responsibilities towards security. Our CAP1224 Accountable Managers document will be beneficial here.

You should immediately notify your Lead Auditor of the change so that they can arrange for a representative from the CAA Senior Management team to conduct an Accountable Manager meeting with the new Accountable Manager.

You should also ensure that this change is captured within the SPD quarterly submissions as part of the Phase 2B process.

Risk Based Oversight (RBO)

What is Risk Based Oversight?

Risk Based Oversight is defined as follows:

“A process which provides the regulator with the means to adjust the scope, frequency and type of its compliance monitoring activities dependent on the entity’s Risk Management and performance profile and the ongoing assurance of their approved internal quality control measures.”

How will the transition from existing compliance monitoring to RBO be managed by the CAA?

The CAA will develop its approach in collaboration with DfT and industry colleagues, and an Industry Working Group will play an important role in this. SeMS principles are closely aligned with those of Safety Management Systems (SMS), so we are also collaborating internally with our SMS colleagues in order to utilise their experience and learning gained from implementing SMS and more widely risk based oversight. We will share details of developments in due course.

What will CAA oversight be like once my organisation has implemented a SeMS?

The long-term approach to oversight in a SeMS environment continues to be developed.

The CAA’s compliance oversight of an entity implementing a SeMS will continue as standard for the foreseeable future. However, we are actively engaging with industry and CAA colleagues to consider how we might begin to plan the transition to a more risk-based approach. It is anticipated that in the future when an entity reaches Phase 2B, i.e. when an entity’s SeMS is confirmed as Operating and Effective, and the CAA receives regular assurance of this, that the CAA will then utilise both SeMS and compliance data to assess whether it may adjust its oversight regime for that entity. We will communicate developments in due course.

Will current compliance observations, audits and inspections still be carried out under a RBO regime?

Current compliance activities will continue until such time as the UK can amend its approach in consultation with industry and other national and international bodies. SeMS oversight is in development, and will run in parallel to our current compliance monitoring regime when an entity’s SeMS is assessed as Operating and Effective, providing continuity and learning. Even within a SeMS environment there will still be a need for a certain level of compliance observations, however, these will follow a more targeted approach over time.

As a SeMS entity, when would we see reductions in compliance activity?

This would be dependent on the CAA receiving assurance that the information provided by an entity about their SeMS is an accurate reflection of your security performance.

Once an entity has achieved Phase 2 status, it will move into Phase 2B, at which point it is required to start submitting regular data sets evidencing that its SeMS continues to be Operating and Effective. The CAA may then use this data, in conjunction with the data from the SeMS Assurance Assessments, as well as compliance data, compliance observations and inspections, to inform a more targeted approach to our work; focusing further on areas of greater risk and/or further areas of concern. It is hoped that this approach will lead to greater collaboration between the Regulator and industry, and facilitate enhanced aviation security performance across the UK, an area which we are working through and due to further explore and develop as we look at data and alike.

Miscellaneous

Does SeMS relate to a whole company, or only part?

The SeMS Framework is aimed at entities that are directed under Civil Aviation legislation. However, should an entity have other sections, subsidiaries and/or sister companies that are not involved in directed aviation security functions, they may choose to implement SeMS principles there as well, as part of a joined-up company-wide approach. These areas would not, however, be monitored as part of the CAA's SeMS programme.

Other transport modes and industries that have a security function or responsibility are also utilising the CAA's SeMS Framework, demonstrating how flexible SeMS can be across all modes of industry, not just aviation.

Will SeMS override Security Programmes?

No, that is not the intention. The requirements of Aviation Security Regulation still apply, however, an entity may choose to combine their SeMS and Security programmes, as has already been done by some.

Can we align the SMS and SeMS terminology? Same words are sometimes used in a slightly different context.

At present there is a need for distinction as we develop SeMS, but in time terminology may be reviewed and aligned where appropriate, using the SeMS Industry Working Group as a forum for consultation.

Will there be changes to the CAA Compliance Teams to reflect a joined-up Safety/Security approach?

There are no plans to combine the CAA Safety and Security functions, as these are two distinct functions governed by different sets of Regulation. However, we are working to develop a more integrated approach to how we conduct oversight of an entity. In practice this means that in the future both safety and security elements will be considered alongside each other, as well as other relevant factors such as licensing, economic, consumer or legal matters.

Is SeMS linked to HMRC Authorised Economic Operator (AEO) status?

Not directly, but we have heard from entities who are embarking on SeMS that the latter has assisted in applying for AEO status, as it provides HMRC assurance on security, compliance and governance.

If my organisation is ISO certified can it be considered to have an Operating and Effective SeMS without the need for a Phase 2 Assessment?

There is no doubt that ISO requirements can complement your SeMS and may well be beneficial to its development. It is worth noting, however, that achieving compliance with ISO9001 does not necessarily mean that you are operating an effective SeMS. This can only be determined by way of a Phase 2 Assessment conducted by the UK CAA.

This is also true for ISO 27001, which relates to the requirements for an Information Security Management System: while we would see ISO 27001 as a positive move and complementary to your SeMS, an entity which is ISO27001 compliant is not considered to have an Operating and Effective SeMS.

Are any other Agencies involved in SeMS?

Not directly, but police, HMRC etc. may be involved in the SeMS process by virtue of their presence on RAG and SEG Committees, for example.

IATA has developed a SeMS for their Members and we are committed to ensuring that the UK CAA SeMS and the IATA SeMS remain closely aligned and continue to complement each other.

How does SeMS relate to SMS? We have an integrated Safety and Security Management System.

SeMS principles are closely aligned with the principles of SMS, but the focus remains squarely on security. We would not discourage an entity from developing a joint SeMS/SMS approach, as long as the SeMS Framework requirements can be clearly evidenced – and indeed, this approach has been successfully taken by some organisations already. However, an entity must be sure that any SeMS-related data requests can be easily ‘extracted’ from a joint approach.

Some entities are now taking a wider view, and considering implementing an Integrated Management System, or IMS, which can enable an entity to integrate all of its systems, processes and standards (such as SeMS, SMS, QMS, ISO etc.) into a single, unified framework and utilise their resource more efficiently and effectively.

What is the view of SeMS beyond the UK?

We are proud to say that the UK aviation industry’s implementation of SeMS has had a significant influence on worldwide thinking and overall development. Since the UK pressed ahead with rolling out SeMS, there has been a lot of interest from ECAC and indeed many other fora. Our progress is watched closely by several states and non-UK entities and we actively engage with other National Aviation Authorities.

ICAO supports the SeMS principles, and the ICAO Secretariat has described the UK SeMS Framework as the first practical exposition of previously theoretical material. The SeMS Framework has been well-received internationally and has been complimented as an exposition of SeMS principles. Our continued engagement with IATA also gives us further insight that we are collaboratively developing SeMS internationally.

How do I assess my Security Culture?

Security Culture is very unique and personal to the entity itself. One approach may not suit all, so it is important that, when looking at Security Culture, this be tailored to what works within your organisation. A positive security culture encompasses all business areas, not just security, so it is vital that all staff are a considered. Assessing a security culture should become routine and we have provided a Security Culture Self-Assessment Tool which may be of use and can be found here https://www.caa.co.uk/Commercial-industry/Security/Security-management-systems/Security-culture-self-assessment-tool/.

There is also further information on Security Culture from ICAO which can be found through the following link: https://www.icao.int/Security/Security-Culture/Pages/default.aspx