Civil Aviation Authority

Security Management System (SeMS)

Frequently Asked Questions

CAP1297

Industry FAQs Index

Why, What, How?

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 organized, systematic approach and effective measurement of its security performance, including 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 under-estimated. Reliance on compliance with the regulations is not enough. Previously unrecognised threats already exist and new threats emerge frequently; and even if there were no such threats, the CAA's oversight is not enough to assure constant compliance – it can only verify compliance at a specific place at a specific time and draw inferences, often not backed by evidence about the other places and times.

Therefore organisations should be alert constantly and searching for threats, especially threats that the regulations do not cover or that the regulations cause. Equally important, once identified these threats and consequent risks need rigorous assessment so that adequate but proportionate and achievable mitigations are designed and implemented.

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

What is the SeMS Framework?

The DfT and CAA have both stated that adopting a SeMS is not mandatory, but if an entity expects the CAA to be able to use its SeMS outputs for oversight, that SeMS must have the components identified in the SeMS Framework. So the Framework can be regarded as the specification, albeit at high level, of an effective SeMS. It describes the ten components without prescribing how an organisation is to implement them.

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 outline guidance on implementing a SeMS. This summarises the key points of the Framework and the CAA's approach to supporting the ongoing industry roll-out of SeMS as well as outlining how an implementation project could be organized. It is the aim of the CAA to avoid prescriptive 'requirements' wherever possible

We have a mature and integrated risk management system already. Is it worth us signing up for SeMS now, are there benefits, or should we wait?

SeMS places accountability for security where it should be – at Board level. Current experiences in implementing the CAA's SeMS framework has shown the following benefits:

- Creates Board level accountability for security
- Enables the Board to monitor compliance with AVSEC requirements, including Regulation (EC) 300/2008
- Demonstrates discharging of accountability and responsibilities for security.

[1] https://www.caa.co.uk/application.aspx?catid=33&pagetype=65&appid=11&mode=detail&id=6543

[2] https://www.caa.co.uk/application.aspx?catid=33&pagetype=65&appid=11&mode=detail&id=6544

[3] http://www.caa.co.uk/application.aspx?catid=33&pagetype=65&appid=11&mode=detail&id=6632

- Encourages transparent and verifiable security
- Delivers greater visibility of compliance assurance
- Enables more effective use of existing tools and systems
- Supports threat assessment methodology
- Builds on SMS learning
- Encourages collaborative approaches
- Empowers and promotes security culture and pro-active reporting
- Drives a more assurance based regime

By starting the SeMS journey now an entity can influence how SeMS develops and share expertise and best practice to the benefit of all.

Is SeMS compulsory?

SeMS is not mandatory, but the CAA can only adjust its oversight arrangements for those organisations with a recognised SeMS – i.e. one that the CAA can verify is delivering dependable results. See also “What will Oversight be like in a SeMS environment?”

Is SeMS suitable for IFS and Cargo?

The SeMS Framework was designed to fit all sectors and development was guided by a cross-industry group. It has been proven in airport, airline and cargo sectors and is indeed being adopted by IFS entities.

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

The Framework was designed to be scaleable to all sizes of organisation. The degree of detail and record keeping is for an organization to determine, based on its SeMS needs. For example in a very small organization the accountable manager may also be the owner of the business and/or responsible for delivery. In such cases the communication and culture change, and performance measurement will clearly be simpler than for large organisations. The ability of SeMS to be used by a smaller organization has already been proven by one of the Pathfinders.

How do we go about implementing a SeMS?

We recommend treating this as a project with time set aside for dedicated, if not full time, resource. The key steps are:

- *Confirm Management Commitment*

Before the project gets too far, the commitment of top management should be secured.

- *Conduct a Gap Analysis*

It is essential to have a good understanding of the organisation’s current processes and systems so that areas where additional work is needed to meet the requirements of the SeMS Framework can be identified.

- *Establish initial performance metrics*

If existing metrics are suitable, the measurement, reporting and governance arrangements for them should be put in place early.

- *Plan the Project*

A Gap Analysis will enable a realistic plan to be created, and ensure that the resources are matched to priorities. The project plan should focus on the three themes of Risk Assurance, Performance Assurance and the Management System.

- *Execute Project Plan*

Normal project disciplines should ensure the project is delivered to plan, although it should be expected that the plan will change as the project progresses.

- *Phase 1 Assessment – SeMS is Present and Suitable*

When the organisation is ready (typically 6 – 12 months after starting if there is a dedicated project manager), the CAA will conduct a Phase 1 Assessment to ascertain whether the SeMS is "Present and Suitable".

- *Phase 2 Audit – SeMS is Operating and Effective*

Following a successful Phase 1 Assessment, the organisation will continue its SeMS project into Phase 2, developing the SeMS to an Operating and Effective state in which it is using it to manage security, and building up performance data and governance records that provide assurance of this.

At that end of Phase 2 the organisation will have built up evidence that the SeMS is operating and that its Risk Assurance, Performance Assurance and Management System are all effective. At that point (perhaps 12 months from the successful Phase 1 Assessment) the CAA will conduct a Phase 2 audit.

For more detail, **see CAP** 1273 "Implementing **SeMS:** An Outline"[4]

Who should I speak to?

Contact the SeMS Team at sems@avsec.caa.co.uk.

It is envisaged that, In the future, your normal CAA compliance contact will be your SeMS contact too.

[4] http://www.caa.co.uk/application.aspx?catid=33&pagetype=65&appid=11&mode=detail&id=6632

Data requirements

What metrics does the CAA expect us to provide?

These are under development, and trials are commencing with Pathfinder entities. There has been a good deal of work undertaken to ensure that these are targeted, meaningful and not onerous to gather. It is not the intention to impose additional burdens on industry, rather to adopt existing metrics that most entities will already be collating.

Performance data – how can we address this requirement if we do not have much to show as yet?

Clearly SeMS data will accrue over time, and the CAA recognizes this. The CAA does not wish to create data sets for their own sake, as they must be meaningful to both the CAA as well as the entity. The size and nature of an entity is taken into account when SeMS oversight is considered.

Generic data - are we looking for standard descriptors?

For the generic sectoral datasets we are looking for data that all can understand and that are comparable within sub-modes. Within an entity's own SeMS, you can choose your own descriptors and these can be used internally, provided they work within the SeMS Framework and are comprehensible and meaningful.

CAA oversight under SeMS

ow will the move from existing compliance activity to SeMS Oversight be managed by the CAA?

The need for a "Phase 3" for SeMS has been identified in order to effectively manage the transition. This is being discussed and developed with industry

What will CAA Oversight be like in a SeMS environment?

The long-term approach to oversight in a SeMS environment continues to be developed. In broad terms it will be as follows.

The CAA's compliance oversight of entities engaged on SeMS will continue as now, until a SeMS is operating and effective.

When the SeMS is providing reliable and accurate data, the CAA will be able to use that data for some aspects of compliance assurance, and in turn adjust the focus of its visits to look at areas of concern. A reliable SeMS will also better inform the CAA's view of any non-compliances – are they one-off or systemic? – and the rectification required.

Oversight at this stage will include audits of the SeMS itself to verify its effectiveness.

In concert with industry, the CAA is working up generic SeMS performance datasets for each sector to enable effective comparisons to be made and to identify any trends that may appear.

As a SeMS adopter, when would we see reductions in Compliance activity?

This depends on the CAA being assured that the information provided by your SeMS is an accurate reflection of your security performance.

Another FAQ (How do we go about implementing a SeMS?) explains the structure of a SeMS project and its two phases. At the end of Phase 2, the SeMS will have built up evidence that it is operating and that its Risk Assurance, Performance Assurance and Management System are all effective. At that point the CAA will conduct a Phase 2 audit. If that is successful, the CAA will commence requesting specific data sets from the entity. This data will be used, in conjunction with results from its onsite visits, to allow for a more targeted approach to its work; focusing on areas of higher risk or areas of concern; It is hoped that this approach will lead to a more collaborative way of working between the regulator and industry, helping develop and improve aviation security across the UK.

Will compliance observations still be carried out under a SeMS regime? Won’t this be confusing?

Normal compliance activities will continue until such time as the UK can amend its approach in consultation with the EC. SeMS oversight is in development, and will run in parallel when an entity’s SeMS is assessed as Operating and Effective, providing for 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.

SeMS outside the UK

What is the view of SeMS beyond the UK?

There has been interest in SeMS at ECAC and other fora. The UK has pressed ahead with rolling out SeMS and this is being followed closely by several states and non-UK entities.. The Framework has been well-received internationally and has won compliments as a good exposition of SeMS principles. ICAO support SeMS principles, and the ICAO Secretariat has described the UK SeMS Framework as the first practical exposition of previously theoretical material. The UK industry's implementation of SeMS is having a significant influence on worldwide thinking about SeMS.

Will Brexit affect SeMS?

It is not anticipated that Brexit will affect SeMS as it is a UK-driven initiative.

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, there is nothing to stop these adopting SeMS principles, thus providing a joined-up approach company-wide. These would not, however, be monitored as part of the CAA's SeMS programme. Other transport modes and industries that have a security function/responsibility have also picked up and are utilizing the CAA's SeMS framework, showing that, with the word aviation removed from the document, this framework does work across all modes of industry.

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

SeMS closely follows the principles of SMS, but the focus is on security. There is nothing to prevent an entity from developing a joint SeMS/SMS approach, as long as the SeMS Framework requirements are clearly evidenced – indeed, this approach has been taken by some already. It would also be necessary to ensure that any SeMS-related data requests were easily 'extracted' from a joint approach.

Is there any benefit in combining a Safety and Security Risk Register?

This can be done, as long as the appropriate risks are clearly identified, actioned and evidenced.

Will SeMS override Security Programmes?

No, that is not the intention. The requirements of AvSec Regulation still apply, although there is nothing to stop an entity combining 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 sometimes a need for distinction as we develop SeMS, but over time terminology can be reviewed and aligned where appropriate, using the SeMS Industry Working Group as a forum for decision.

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.

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

Currently there is no capability to do this, and any plans to combine Safety and Security functions, even at the basic level, would need to be looked at some time in the future.

Are any other Agencies involved in SeMS?

Not as such, but Police, HMRC etc. are getting involved in the SeMS process by virtue of their presence on RAG, SEG Committees, for example.

What do you see as the biggest challenge in SeMS?

The move from a “direct and inspect” regulatory regime towards more self-assurance by industry is, of course, a challenge. This requires a cultural and attitudinal change both by industry and the regulator. However, we are confident that this can be achieved, and SeMS is making good progress to date.