Department
for Transport

UK
Civil Aviation
Authority

Implementing a Security Management System (SeMS): An Overview

CAP 1273

Published by the Civil Aviation Authority, 2021

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

First published 2014
Second edition 2018
Third edition 2021

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP1273

The purpose of a Security Management System

The purpose of a Security Management System (SeMS) is to enable an entity to identify and manage its security risks and be assured right up to Board level that the security measures taken to manage those risks are effective.

Current regulatory compliance activity, such as observations and inspections, cannot provide an entity with the continuous assurance of the performance of its security measures. The combination of governance, threat and risk management and performance measurement, achieved through a SeMS, can provide that assurance. It is a system with many similarities to quality management systems.

In essence, a SeMS provides the necessary organisational structure, accountabilities, policies and procedures to ensure effective security oversight.

SeMS Principles

A SeMS will provide an entity with a structured approach to managing security as an integral part of their overall business. It also serves as a tool for systematically integrating security risk management into an entity's day to day operation in close alignment with other risk management systems such as Safety Management Systems (SMS). The concept is that:

- security risks are **managed at the right level**, overseen by company boards
- **activities are measured** to provide management information on security performance;
- there are people in the entity who are **accountable** for maintaining rigorous security standards, using the management information; and
- there is a positive security **culture** that promotes high-security standards throughout the entity.

SeMS in practice

A SeMS requires several practical components to be in place. Many of these may already exist within an entity but may need to be made more robust, reliable, consistent, repeatable, and effective. A SeMS is a practical approach to assessing these components and removing loopholes, vulnerabilities, gaps and duplications.

An entity could work out the components of a SeMS by analysing what would be required to *"identify and manage security risks and be assured that the security measures are* *effective”*. However, in collaboration with Industry, the SeMS Framework[1] has been developed to save entities from starting from first principles. The CAA and DfT designed the SeMS Framework to deliver a degree of consistency across Industry, regardless of the size or nature of the business.

The Framework consists of ten chapters describing the components of a SeMS. A simple way to appreciate the contents is to group the ten chapters into two themes:

Corporate Assurance	Chapter 2: Threat and Risk Management
	Chapter 5: Performance Monitoring, Assessment and Reporting
The Management System	***Culture and Accountability*** Chapter 1: Management Commitment Chapter 3: Accountability and Responsibilities Chapter 9: Security Education Chapter 10: Communication ***Enablers*** Chapter 4: Resources Chapter 6: Incident Response Chapter 7: Management of Change Chapter 8: Continuous Improvement

The effectiveness of the SeMS will depend significantly on the relevance and active presence of the entity's performance monitoring. Therefore, the entity must ensure that the Threat and Risk Management and Performance Monitoring, Assessment and Reporting chapters are coordinated accordingly. These two chapters give the entity the confidence that mitigation measures are implemented for all identified threats and risks and are achieving their intended objectives.

[1] CAP1223 (Framework for and Aviation Security Management System) and CAP1224 (SeMS - A Guidance Note for Accountable Managers), available from the CAA website.

Performance Assurance

An entity needs to know whether its security processes are functioning correctly and that its investment in security is delivering adequate and meaningful returns. In addition to the data required to demonstrate compliance against regulations, each entity will collect data specific to its security operation. Security measures are integral to the mitigations in place to address specific threats, and so knowing how effective they are is essential for assuring the overall security picture.

An entity will need to precisely establish what it should measure to gain a comprehensive picture of the state of its security and its compliance against regulations. In effect, the entity will need to develop metrics[2], giving each management level the required information about security performance. Data that feeds into the metrics will come from many sources, such as observations, internal and external tests, audits, and records. Metrics could take three forms:

Quantitative	Metrics that check whether tasks are carried out as often as they should be or at the right time of day, etc. For example, whether sufficient vehicle checks are conducted or whether recurrent training is delivered before it expires.
Qualitative	Metrics that check whether tasks are completed to the required standards or whether equipment is functioning to the required standards. For example, observations of searches or checks of equipment performance.
Output	Metrics that capture the outcomes or outputs that are being delivered. For example, the results of covert tests results or TIP data.

The collection of quantitative performance data is a necessary part of a SeMS. However, to be satisfied that all planned security activities are conducted, only the collection of qualitative data and outputs will inform management that their investment in a security system delivers the required results. This complete picture will then enable the entity to address any failings.

When the SeMS is producing meaningful data on its performance against regulatory requirements, and those specific to its local operation, and has processes in place to quality assure this data, it can then be used by the Regulator to contribute to an overall

[2] The term “Metric” is used in this document to signify any measurable indicator of performance. The term “Measure” is used to refer to security protection or risk mitigation actions.

picture of compliance for that entity. For that reason, this data must be honest and accurate; otherwise, it compromises the SeMS and overall security compliance.

It is essential that the duration of time that security performance data will be kept for is defined and that the data is stored securely and in a way that makes it easy to access and process.

What about smaller entities?

The same principles apply. A smaller entity will still need to know how it is performing against regulations and its security targets. However, collecting and analysing security data can be very straightforward and captured using a single spreadsheet .

Risk Assurance

For the performance monitoring to be relevant to the entity, the Threat and Risk Management process must be robust and effective. However good the performance, unless efforts are focused on the right risks and issues, security cannot be assured.

Although entities are advised of national and international threats by the government, they will want to identify any local threats which could affect their operation. For example, an airport may be the target for activists opposed to expansion, or a cargo agent may be vulnerable to theft. All such local threats need to be identified and risk assessed (which includes identifying where the vulnerabilities lie) to allow the appropriate mitigation to be put in place.

Many larger entities are likely to have well-established threat and risk assessment processes in place and can ensure these include locally identified threats. These additional threats, once assessed, should be entered into the entity’s risk register, together with the relevant mitigations. The risk will never be reduced to zero; therefore, there needs to be senior management acceptance of the residual risk – i.e. acknowledgement that the mitigations are adequate – and continuing awareness of how well the mitigations are performing.

What about smaller entities?

The principle is the same for smaller entities, but in practice, some small entity may not have a formal threat and risk assessment process with a risk register. However, it will still need to have a way of identifying and dealing with any local threats, which could involve being aware of local crime trends in its neighbourhood and receiving regular updates from the local police, for example.

The Management System

Incorporated within Performance Assurance and Risk Assurance are several enabling mechanisms that make up the “Management System” for security.

Culture and Accountability

A SeMS entity will exemplify a positive security culture, led from the top and inherent in the actions and behaviours of all personnel at every level within that entity. The level of attention, commitment and support that senior management gives to security should be comparable to that given to other key corporate activities. If management is committed to SeMS and demonstrates that commitment, this will set the standard for a strong security culture. One tangible way of demonstrating management commitment is by communicating a security policy that embodies the SeMS ethos of the entity and makes security everyone’s shared responsibility. A security policy is the written evidence of Senior Management’s commitment to delivering effective security.

Through the development of a positive security culture, all staff members will become aware of their security roles and responsibilities and the decision-making process. Job descriptions, personal and business targets, education and training, should define and explain these accountabilities and responsibilities. While clearly defined governance groups, processes and information will provide suitable terms of reference.

Enablers

Resources must be sufficient and suitable. Through the SeMS, the entity will establish the correct level of resources and ensure these resources are appropriate for the task. For example, in the case of security staff, a recruitment process determines if the candidate has the necessary aptitude for the job, and the training equips them with the required skills. Third-party suppliers are also part of an entity’s resource and must feature within the SeMS. The entity should define, within their SeMS, responsibilities for managing any such outsourced security-related service(s), including quality assurance of the activities that the third party is providing. It is essential to remember that the ultimate responsibility of the security service(s) provided lies with the entity and is ever more critical in the level of oversight activity that the entity conducts internally.

A security incident could have a significant impact on the ability of the entity to continue its operations. In order to appropriately prepare for dealing with any such event, the entity should have defined security response procedures, so it can mitigate the impact and recover swiftly from any disruption.

Changes to operational processes, resources or tools may inadvertently compromise security. There should be a defined change management process that identifies all internal and external changes and assesses any security impacts or risks for each of them.

Continuous improvement is not so much a process; instead, it is the creation of an environment where continuous awareness of performance and the pursuit of improvement are the norms. The SeMS will present a flow of security performance information to those responsible for security within the entity. How the entity acts upon that information is at the heart of a SeMS. The entity should seek to build on its strengths and encourage honest discussion about how to remedy poor performance, and identify and implement necessary improvements. Any overall improvement will also contribute to enhancing the entity's resilience.

SeMS Implementation Guidance

Treat this as a programme of activity, with time set aside for sufficient resource.

There is a relatively short burst of activity (typically 6 to 12 months – depending on entity size) to create the initial SeMS Phase 1 - Present and Suitable. Following this stage is Phase 2 – Operating and Effective, where the entity will implement and embed the SeMS into their daily operations. Throughout the initial phases, the entity must give sufficient resources and focus to the programme in order to sustain momentum.

Follow a step by step approach (although the sequence of the first four steps can be altered and depends on an entity's approach and existing structures):

Management Commitment

Before the programme commences, the entity should secure a commitment from senior management. The resource for the SeMS programme is likely to require senior management approval and the protection from interference or distractions that this should guarantee. The changes in culture and ways of working that the programme will bring will require endorsing and commitment from the top so that the senior commitment to SeMS is clear.

Gap Analysis

It is essential to have a good understanding of the entity's current processes and systems to identify areas where additional work is needed to meet the SeMS Framework requirements. Without that, the management commitment represents only blind faith, not an informed choice.

Establish initial Performance Metrics

If existing metrics are suitable, the measurement, reporting and governance arrangements for them should be put in place early. This demonstrates tangible delivery of the programme and starts to build a performance culture. For airports, TIP data is one prime example of such a metric.

Plan for the SeMS Implementation

A Gap Analysis will enable a realistic plan to be created and ensure that the resources are matched to priorities. Again, management commitment can only be verified when the resources, finances and management costs are understood and provided for the programme.

Execute the Plan of Activity

Standard programme disciplines should ensure that implementation is delivered to plan, although it should be expected that the plan will change as the programme of activity progresses. The plan, or the revised plan, will ensure all the right actions are taken at the right time with the right resources. Additional care and attention is needed to ensure that sufficient dedicated time is allocated to each of the roles that are involved and critical to the success of implementation.

CAA Support

Once the entity expresses an interest in implementing a SeMS, they will be invited to attend the SeMS Industry Working Group (SIWG). At the SIWG, the entity will engage with other industry members who are embarking on their SeMS programme, and the CAA will provide delegates with updates, advice and guidance on implementing and embedding a SeMS. In conjunction, a CAA auditor will guide the entity through the different phases of the SeMS. The SeMS process is as follows:

Phase 1 Assessment – SeMS is Present and Suitable

When the entity is ready (typically 6 – 12 months after starting with a dedicated programme manager), the CAA will conduct a Phase 1 Assessment to ascertain whether the SeMS is “Present and Suitable”. For example, the CAA will review the SeMS to verify it is to the required Phase 1 standard, the Accountable Manager is appropriately senior and has demonstrated a commitment to the programme and the ongoing SeMS. As part of the assessment, a member of the CAA Senior Management team will hold an informal interview with the entity’s Accountable Manager.

Phase 2 Assessment – SeMS is Operating and Effective

Following a successful Phase 1 Assessment, the entity will continue its SeMS programme into Phase 2, developing the SeMS to Operating and Effective. The entity uses the SeMS to manage security and build up performance data and governance records that assure this.

Throughout Phase 2, the allocated member of the CAA SeMS Operational Team will liaise with the entity to assist in building up evidence to meet the Phase 2 criteria.

Once the entity has built up evidence that the SeMS is operating and effective (perhaps 12 months from the successful Phase 1 Assessment), the CAA will conduct a detailed Phase 2 Assessment. The aim is to identify if the entity effectively manages security through the documented formal processes detailed in the entity's Phase 1 Assessment. The CAA will also validate that the entity is producing and using the relevant outputs from the SeMS. To summarise, Phase 2 seeks to confirm that there is an Operating and Effective SeMS in place. As part of this, a CAA Senior Manager holds a formalised meeting with the entity's Accountable Manager.

Phase 2B – Continued Assurance of the SeMS

At Phase 2B, the entity provides continued assurance of their SeMS to the CAA, which comprises of quarterly submissions of SeMS Performance Data (SPD) to the CAA. To complement SPD submissions, the CAA will conduct an assurance site visit to verify the SeMS continues to be operating and effective. During this visit, the entity will have the opportunity to provide documented evidence to demonstrate that its SeMS continues to operate effectively and fulfils all chapters of the SeMS framework document. The CAA will also conduct additional operational assessments across the entity's site(s) as part of the Phase 2B assurance process.

Future Regulatory Reform

A Risk-Based Oversight (RBO) regulator effectively utilises data to adjust the scope, frequency and type of compliance monitoring activities, leading to a further efficient, risk-based oversight regime.

The UK CAA is currently working with Industry to develop a RBO approach for Aviation Security. SeMS is the necessary precursor for the CAA to introduce a RBO programme. The CAA must identify the most appropriate data sets for the basis of adjusting its oversight regime. Assurance of security performance through SeMS is essential for the CAA to build its data set and evidence base for remodelling oversight.

Therefore, for an entity, developing an effective SeMS in line with the SeMS Framework should, in time, offer an entity the prospect of adjusted scope, frequency and type of regulatory observations and inspections, leading to a more risk-based approach to compliance oversight from the CAA