Department for Transport

Civil Aviation Authority

# Implementing a Security Management System: An Outline

CAP 1273

CAA House, 45-59 Kingsway, London WC2B 6TE
www.caa.co.uk

# 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 continuous assurance of the performance of its security measures. The combination of governance, threat and risk management and performance measurement that alone can provide that assurance equates to a SeMS. It is a system, with many similarities to quality management systems.

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

# SeMS in practice

To realise that concept, the 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 rigorous, reliable, consistent, repeatable, and effective. The SeMS project discussed below is a practical approach to assessing these components and removing loop-holes, weaknesses, 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" (the goal outlined above). However, the SeMS Framework has been developed in conjunction with industry to save entities having to start from first principles. It is also designed to deliver a degree of consistency across the industry, regardless of size or nature of the business, e.g. airport, airline, cargo or in flight supplies.

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 three themes:

| | |
|---|---|
| Corporate Assurance | Chapter 2: Threat and Risk Management |
| Risk Assurance | Chapter 5: Performance monitoring, assessment and reporting |
| The Management System | ***Culture and Accountability***<br>Chapter 1: Management Commitment<br>Chapter 3: Accountability & responsibilities<br>Chapter 9: SeMS Education and Security Culture<br>Chapter 10: Communication<br>***Enablers***<br>Chapter 4: Resources<br>Chapter 6: Incident response<br>Chapter 7: Management of change<br>Chapter 8: Continuous improvement |

It is in Performance Monitoring, Assessment and Reporting where consistency across the industry is vital for SeMS to work nationally. But in order for the performance monitoring to be relevant to the entity, the Threat and Risk Management must be rigorous and effective. These two chapters therefore need more coordination across entities than the remaining eight Management System chapters.

## Performance Assurance

An entity needs to know whether its security processes are functioning correctly and that its investment in security is delivering effective returns. In addition to the data required to demonstrate compliance against regulations, each entity will want to collect data specific to its own 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.

In order to gain a comprehensive picture of the state of its security and its compliance against regulations, an entity will need to establish exactly what it should be measuring; in effect it will need to establish metrics which will give each level of management the required information about security performance. Data which feeds into the metrics will come from many sources, and will include observations, tests, audits, checks of records etc. Broadly speaking metrics could take three forms:

| | |
|---|---|
| Quantitative | Metrics that check whether tasks are being carried out as often as they should be or at the right time of day, and so forth. For example, whether sufficient vehicle checks are being carried out or whether recurrent training is being given when it is due. |
| Qualitative | Metrics that check whether tasks are being carried out 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. |

Whilst the collection of quantitative performance data is a necessary part of a SeMS, in order to be satisfied that all planned security activities are being carried out, it is only the collection of qualitative and output data that will inform management whether their investment in security systems is delivering the required results. This complete picture will then enable the entity to address any failings.

Once an entity's SeMS is producing meaningful data on how it is performing against both regulatory requirements and those specific to its own local operation, and is enabling it to demonstrate that it has processes in place to quality assure this data, then this SeMS can be used by the Regulator to contribute to an overall picture of compliance for that entity. It is, of course, vital that this data is honest and accurate, otherwise the SeMS is compromised.

However an entity chooses to collect, compile and record security performance data, it is important that the duration of time that data will be kept for is defined and that the data is stored both securely and in ways which make it is easy to access and process.

### Consistency of Metrics

The CAA will use selected metrics from each entity to inform its oversight of the entities themselves and also of the mode as a whole. Metrics may differ to some degree from one entity and mode to another, and it is clearly impossible for the CAA to reconcile and process hundreds of different types of metric. We are therefore working with industry to define a standard core set of consistent performance metrics, to facilitate meaningful modal trend analysis. This will also enable the CAA to inform the entity how well its own performance compares to the modal benchmark generally.

This consistency is important if the CAA is to be able to use the related SeMS metric results as part of its regulatory oversight: without it neither the entity nor the CAA will gain the full benefits of SeMS and the focus of the CAA's regulatory oversight will remain on existing levels and methods of compliance activity.

As an example, the first such set of standard core metrics for airports could be Threat Image Projection (TIP) data. Note that this is mandating neither TIP nor SeMS: it is simply requiring those entities who wish their SeMS to be used by the CAA as part of its compliance oversight to ensure the outputs are consistent with a standard core set.

### What about smaller organisations?

Exactly 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 should be much simpler and could involve nothing more complicated than a single spreadsheet.

## Risk Assurance

In order for the performance monitoring to be relevant to the entity, the Threat and Risk Management must be rigorous and effective. However good the performance, unless it is focused on the right risks and issues, security cannot be assured.

Although an entity will be advised of national and international threats by the government, it will want to identify any local threats which could affect its 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 then 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 the locally identified threats. These additional threats, once assessed, should be in the entity's risk register, together with the relevant mitigations. Risk will never be reduced to zero, and there needs to be senior management acceptance of the residual risk – i.e. acknowledgment that the mitigations are adequate – and continuing awareness of how well the mitigations are performing.

### What about smaller organisations?

For smaller entities, the principle is the same but in practice a small entity is unlikely to have a formal threat and risk assessment process with a risk register. It will still need to have a way of identifying and dealing with any local threats, which could for example involve being aware of local crime trends in its neighbourhood, and receiving regular updates from the local police.

## The Management System

Wrapped around Performance Assurance and Risk Assurance there will be several enabling mechanisms, which together make up the "Management System" for security.

### Culture & accountability

For SeMS to work, a culture of security, emanating from the top of the entity, should be inherent in the actions and behaviours of all the people, at every level. 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 the 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 which embodies the SeMS ethos of the entity and makes security everyone's shared responsibility. A security policy is the written evidence of the entity's commitment to delivering effective security.

In a SeMS culture, all staff throughout an entity will be aware of their security roles and responsibilities, and of the decision-making process. This should be reflected in job descriptions,

targets, education and training as well as clearly defined governance groups, processes and information flow.

### Enablers

**Resources** must be sufficient and suitable. As well as ensuring that the correct level of resources is provided it is important to ensure they are appropriate for the task. So, in the case of the security staff for example, all will have gone through a recruitment process which ensures they have the necessary aptitude for the job, and their training will have equipped them with the required skills. Third party suppliers are also part of an entity's resource, and if the provision of certain services is contracted out, the responsibility for what is being delivered remains with the entity. Any such security-related service will need to be included in the SeMS, and there should be regular quality assurance of what is being provided to ensure that it meets the standards specified by the entity and the relevant regulations.

A security incident could have a major impact on the ability of the entity to continue its operations. In order to ensure that it is properly prepared to deal with any such event, the entity should have a **security response process**, so it can mitigate 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 for each of them any security impacts or risks.

**Continuous improvement** is not so much a process as the creation of an environment where continuous awareness of performance and the pursuit of improvement are the norm. The SeMS will ensure that there is a flow of security performance information being presented to those who have responsibility for security within the entity. How that information is acted upon 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 how to identify and implement necessary improvements. Any overall improvement will also contribute to enhancing the entity's resilience.

# SeMS Implementation Guidance

## Treat this as a project, 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) followed by a (Phase 2) in which the entity will adopt the SeMS and make it effective. This initial work can lose momentum and focus if resources are constantly diverted to other tasks.

## 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 project commences, the commitment of top management should be secured. The

resource for the SeMS project is likely to need top management sanction, and the protection from interference or distractions that this should guarantee. The changes in culture and ways of working that the project will bring will need endorsement from the top, to make the senior commitment to SeMS clear.

### Gap Analysis

It is essential to have a good understanding of the entity's current processes and systems so that areas where additional work is needed to meet the requirements of the SeMS Framework can be identified. 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 by the project and starts to build a performance culture. For airports, TIP data is one prime example of such a metric.

### Plan the Project

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 tested when the financial, resource and management costs of the project are understood and the resources, finances and management time are provided to meet them.

### 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. The plan, or the revised plan, will ensure all the right actions are taken at the right time with the right resources.

When the project manager is also a subject matter expert, care is needed to ensure sufficient dedicated time is allocated to each of those roles.

### CAA Support

A member of the CAA SeMS Team will have been allocated as a liaison point following successful initial questionnaire submission. The SEMS approval 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 project manager), the CAA will conduct a Phase 1 Assessment to ascertain whether the SeMS is "Present and Suitable": is it complete, does it look as though it all works, is the Accountable Manager appropriately senior and has he/she demonstrated full commitment not only to the project but to the ongoing SeMS? An informal interview will be held with the Accountable Manager and a CAA manager.

### Phase 2 Assessment – SeMS is Operating and Effective

Following a successful Phase 1 Assessment, the entity 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.

Throughout Phase 2, the CAA compliance oversight of the entity will continue as before, and in parallel the allocated member of the CAA SeMS Operational Team will liaise with the entity to assist in building up evidence that it will meet 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 is effectively managing security through the documented formal processes set out in Phase 1 and producing and using relevant outputs. In sum, Phase 2 seeks to confirm that there is an Operating and Effective SeMS. As part of this a more formalised meeting will be arranged between the Accountable Manager and a senior manager of the CAA.

### Phase 3 – Transition to full SeMS and CAA SeMS Oversight

The entity continues to use SeMS to manage security and the process matures into business as usual, supported as required by the CAA. During this phase the CAA will look to realign compliance activity insofar as the regulations allow.

# Future Regulatory Reform

When a sufficient number of entities have established an operating and effective SeMS, and reporting against performance measures/indicators is embedded, the CAA will make use of the data it has assembled to identify areas where the regulatory oversight could be more aligned to Better Regulation principles. In doing so it will target both the CAA's oversight of existing regulations, and the promotion of improvements to those regulations.

Whilst it is the intention, once sufficient evidence is available to support change, for the DfT and the CAA to take proposals to the European Commission in respect of wider EU regulations, any such approaches will need to take account of/be governed by Brexit discussions/outcomes.

Further copies of this publication can be downloaded from **www.caa.co.uk**