

# Security Management System (SeMS) Frequently Asked Questions



# Industry FAQs

---

## Why do we need to care about 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 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.

## What Benefits will we get from SeMS?

---

The key benefits are:

- Assurance for the organisation's Board that security performance is good and does not pose a threat to the organisation's reputation
- Rectification can be planned and actioned because the organisation knows the issues before the Regulator finds them – and planned actions are more effective and less costly than those that are reactive.
- Tangible risk prevention – understanding risks and reducing risk likelihood

## What's in it for me?

---

See "What Benefits will we get from SeMS?" Your business will have a much better appreciation of security issues and be better placed to manage and address them in a planned way, rather than a reactive (and usually more costly) manner. You will be able to:

- Better measure and manage security performance
- Better determine the impact on security of all significant business decisions
- Submit meaningful performance reports regularly to the Board
- Provide evidence for discussions on key issues with the Regulator

As a result, the Board will be able to

- Review reporting of performance, risks and issues
- Ensure action is taken to eliminate root causes of deficiencies and reward good performance

- Actively manage security culture and behaviour
- Understand security as a necessary part of business
- Ensure that business decisions include security impact analysis

You will also be able to help shape and influence the journey towards a more performance-based regulatory regime.

## What is the view of SeMS beyond the UK?

Several European countries expressed interest in SeMS at an ECAC SeMS conference led by DfT in 2013. Since then, the UK has pressed ahead with publication of the Framework to form the foundation for rolling out SeMS. The Framework has been well-received internationally and has won compliments as a good exposition of SeMS principles. British Airways intend to propose it to IATA as a model to improve the ISOS audit regime. The chairman of ICAO's Guidance Material Working Group has said he intends to draw deeply on our material them in formulating ICAO's guidance in the SeMS area. The ICAO Secretariat has described it as the first practical exposition of previously theoretical material.

As a result we expect the Framework and the UK industry's implementation of SeMS will have a significant influence on worldwide thinking about SeMS.

## 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?"

## What does the SeMS Framework actually mean?

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 \(CAP1223\)](#) and [Guidance for Accountable Managers \(CAP1224\)](#) the CAA has also published [Implementing SeMS: An Outline \(CAP1273\)](#) to provide outline guidance on implementing a SeMS. This summarises the key points of the Framework and the CAA's approach to supporting industry roll-out of SeMS as well as outlining how an implementation project could be organized.

More detailed guidance may be developed to explain the Framework more fully, if that proves necessary. However the risk is that more detail results in more prescriptive 'requirements' – precisely what the SeMS Framework aims to avoid.