

Implementing a Security Management System: An Outline



© Civil Aviation Authority 2015

All rights reserved. Copies of this publication may be reproduced for personal use, or for use within a company or organisation, but may not otherwise be reproduced for publication.

To use or reference CAA publications for any other purpose, for example within training material for students, please contact the CAA for formal agreement.

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 organisation 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.

Spot checks and regulatory inspections cannot provide the organisation with continuous assurance of the performance of its security measures. The combination of governance, threat and risk management and performance measurements 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 oversight.

SeMS Principles

For security management to be effective, it has to be a continuous cycle which includes a threat and vulnerability assessment, the identification, capture and analysis of risk, and the generation and continuous review of risk mitigation plans. Risk is a dynamic area and will require continual review against an ever changing threat landscape.

A Security Management System (SeMS) achieves these things by providing an organised, systematic approach to managing security which embeds security management into the day-to-day activities of the organisation. 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 organisation 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 organisation.

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, effective or any number of similar adjectives. The SeMS project discussed below is a practical approach to assessing these components and removing loop-holes, weaknesses, gaps and duplications.

An organisation 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 Framework¹ has been developed in conjunction with industry to save organisations having to start from first principles. It is also designed to deliver a degree of consistency across the industry.

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:

Performance Assurance	Chapter 5: Performance monitoring, assessment and reporting
Risk Assurance	Chapter 2: Threat and Risk Management
The Management System	Culture and Accountability Chapter 1: Management Commitment Chapter 3: Accountability & responsibilities Chapter 9: SeMS Training & Education Chapter 10: Communication Enablers Chapter 4: Resources Chapter 6: Incident response Chapter 7: Management of change 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 organisation, the Threat and Risk Management must be rigorous and effective. These two chapters therefore need more coordination across organisations than the remaining eight Management System chapters. The CAA will therefore focus the majority of its SeMS effort on helping organisations ensure that they can deliver against the requirements of those two chapters.

Performance Assurance

An organisation 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 organisation 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 organisation will need to establish exactly what it should be measuring; in effect it will need to establish metrics² which will give each level of management the required information

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

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.