UK Civil Aviation Authority

The Security Management Systems (SeMS) Strategy 2025 - 2030

SeMS Strategy

Key Components of a SeMS

A SeMS should include the following key components:

1. Management Commitment
2. Threat and Risk Management
3. Accountability and Responsibilities
4. Resources
5. Performance Monitoring, Assessment and Reporting
6. Incident Response
7. Management of Change
8. Continuous Improvement
9. Security Education
10. Communication

Executive Summary

Security Management Systems (SeMS) is a framework designed to support entities in managing their risks locally. It does not replace the legal and minimum regulatory security standards and requirements but allows an entity to take ownership of their own risks and meet existing regulatory risk management requirements.

This strategy is designed to signpost the key objectives of the framework in the UK:

- Setting out our vision for SeMS
- Highlighting what we consider to be the key areas where long term maturity will have the biggest impact (must win objectives)
- The practical workstreams that support the implementation of the above (tactical initiatives)
- The enabling capabilities we consider to be key

The basis of the strategic approach is a recognition of the outcome of an operating and effective SeMS – the foundation that underpins the system.

Evolution not revolution

This strategy is the result of a conscious decision by the CAA in 2024 to take stock of the UK's approach to SeMS. The strategy does not intend to change the existing SeMS framework or fundamentally change what SeMS intends to achieve. It does aim to communicate clearly what we see the future of SeMS to be in the UK and where we see the biggest potential for impact.

Target audience

Whilst SeMS does not present a mandated requirement under the UK NASP, its key components are already required: risk ownership, quality assurance and security culture. So, whether an entity is already utilising the UK SeMS framework or has adopted a different approach to local risk management (SeMS in principle), this strategy covers both.

Our vision

Working alongside industry stakeholders, we will support them as they effectively and comprehensively manage their operational security risks. Together we will achieve a more resilient and smarter aviation security system, enabled by technology and human performance, for the benefit of all.

Must win strategic objectives

Key areas where long term maturity will have the biggest impact

Embed Human Factors into our Security Culture

How will we do this? Continue our support to stakeholders for local implementation of a positive security culture, through regulatory measures and guidance.

Support the increased awareness and knowledge of human factors by building human factor principles into our regulations, guidance and workstreams, including as part of SeMS assessments.

Measures of success:

- The inclusion of security culture and human factor principles into an entity's everyday processes at design stage.
- An operating environment which embraces, and role models these principles, and recognises their value.

Enhance risk management capability

How will we do this? We will support industry partners as they enhance their skills, knowledge and confidence in risk assessment and risk acceptance methodologies. We will increase our support to increase capability in building local risk registers.

Measures of success:

- Stakeholders communicate confidently about risk and adopt risk management as an inbuilt approach at their entity.
- Our conversations with entities are centred around risk.

Data integration

How will we do this? Utilise and connect human and system performance data together to drive better security outcomes by identifying system vulnerabilities, human factors and areas for early improvement. We will continue to promote robust quality assurance and quality control processes in support of this.

Measure of success:

- Stakeholders intervene early to resolve developing trends where the security outcome is negatively impacted.

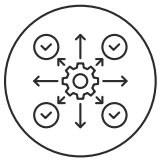
Tactical initiatives

The practical workstreams to support the implementation of the strategic objectives

Alignment

We will:

- Continue to work in close alignment with the other CAA AvSec functions (Compliance, Cyber and Regulation)
- As the CAA evolves its operating model (risk led approach), SeMS remains an integral part of our core service delivery
- We will continue our work with international partners to ensure we reflect best practice



Operating model

We will:

- Optimise our delivery of SeMS to ensure we utilise our resource effectively and efficiently
- Build risk considerations into our oversight (e.g. frequency of visits)

Data analysis

We will:

- Gather the right data for the right audiences and make it available via easy-to-use dashboards
- Analyse and utilise SeMS-related data for the purposes of oversight and management of risk

Training

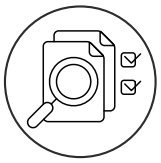
We will:

- Target our internal capacity building and training activities where the most support is required
- Empower stakeholders to build knowledge and skills through the provision of appropriately targeted guidance and training, to include the topic of risk management

Regulatory links

We will:

- Create stronger links between existing regulatory provisions for threat and risks, as well as quality assurance
- Promote SeMS as a vehicle to meet existing regulatory provisions



Root Cause analysis

We will:

- Support the implementation of root cause analysis as part of incident/issue reviews
- Drive stronger links between root cause analysis and effective corrective action, including specifically human factors considerations

Enablers

Key capabilities

How are we delivering these?

- By building our data analysis capability within the CAA and supporting stakeholders to review entity and human performance data
- Being informed by data – having the right systems in place, discovery work to understand how to better utilise data to inform our approach
- Engaging with stakeholders and providing support to empower stakeholders to help themselves

Foundation

Bringing SeMS full circle

Our approach to SeMS is underpinned by a circular approach that is self-reinforcing. SeMS supports the creation of a robust security culture and increases awareness of human factors. It builds capability for managing risks locally and uses this confidence to reinforce the overall system.

SeMS recognises that a systems approach is required to achieve a solid foundation and that building this foundation takes time.