



# SeMS Myths, Fantasies and Fake News: FIVE LESSONS LEARNED

**Andy Blackwell** and **John Wood** have been delivering practical and strategic SeMS (Security Management System) solutions for the past five years. Here they share their experience and expertise.

## Flat earth, 'fake news' and SeMS

Our planet was once believed to be square and stationary; intrepid navigators returned home with fantastic stories of what they had seen (even those that had not actually done any exploring). We are finding the same problems with SeMS: plenty of myths, legends and intrepid navigators, and an abundance of fantasies that tarnish 'brand SeMS'.

Ask "What is a SeMS?" and you will get a myriad of responses, some complex, some irrelevant and many misleading. With so many different things given the name of SeMS, the simplicity and clarity of the SeMS framework can get lost – particularly ironic as the whole point of a SeMS is to give you a 'real' picture of security.

The SeMS framework we refer to throughout this article is the UK Civil Aviation Authority's 'Framework for an Aviation Security Management System' downloadable free from their website (search for CAP1223). Don't be misled by its simplicity: it's comprehensive and highly effective.

This article aims to dispel the myths and share some simple practical examples of the key corporate benefits of a real SeMS. If it reads like a call to action, it is; the need for security assurance and therefore the value of SeMS has never been greater. Once you start your SeMS journey, you'll never look back.

## Myth: SeMS is difficult and expensive

One of the worst aviation security myths is that SeMS is difficult and expensive. The reality is very different: SeMS makes security management easier, as this real-life testimony shows:

You may be thinking that implementing a real SeMS would be difficult, but I can still remember my initial worries having learned that my boss had volunteered the airline to be a pathfinder for the SeMS programme.

- Would it create more work for an already 'pressured' security team?
- Was this just another management fad that would fizzle out and be replaced by something else in time?
- Would this not just duplicate what we were already doing (or thought we were already doing)?
- Would the project distract us from the 'day job' and divert already scarce resources?

Implementing SeMS was a big learning curve for me and the team, but we soon realised that our worries were unfounded, and the effort we invested in the early stages of the project created a more systemised approach to security

and actually made the day job easier.

My lightbulb moment came from a short-notice CAA inspection.

I decided to do the right thing and just 'bite the bullet'. By that I mean no preparation for the audit. If we fast forward, the audit went well, no issues, and it was clear that our more systemised way of doing things made it much easier to locate information and demonstrate that we were in compliance (in reality we were exceeding the mandated requirements where we thought that was necessary).

From that moment onwards I didn't need convincing about the value of SeMS, the concept was now reality for me.

So, despite the common misconception that implementing a SeMS is expensive and requires significant resources, a real SeMS provides a cost-effective solution that builds on existing investment and skills, empowers people and harnesses existing resources. It's not about re-inventing wheels. In fact, most organisations already have many of the SeMS components as security activities, albeit not in a unified system.

Nor is the SeMS complicated. A SeMS is simply an assurance system for security; it doesn't need to be any more complicated than that. A real SeMS minimises complexity yet gives the board

and accountable manager assurance that risks are under control and properly managed. Assurance is important not only for the board, but for the whole organisation, and key stakeholders and customers too.

### So lesson number 1 is...

SeMS is easy and does not have to be expensive

### Myth: You can buy SeMS off the shelf

There are salesmen that tell us they have a SeMS you can buy. Many things get called a SeMS and care is needed to avoid the fantasies. The fact is that off-the-shelf, ready-made solutions are doomed to failure quite soon after the salesman has taken his money. It's very enticing, isn't it? And just look at the business case: guaranteed compliance and elimination of the big risks for no effort.

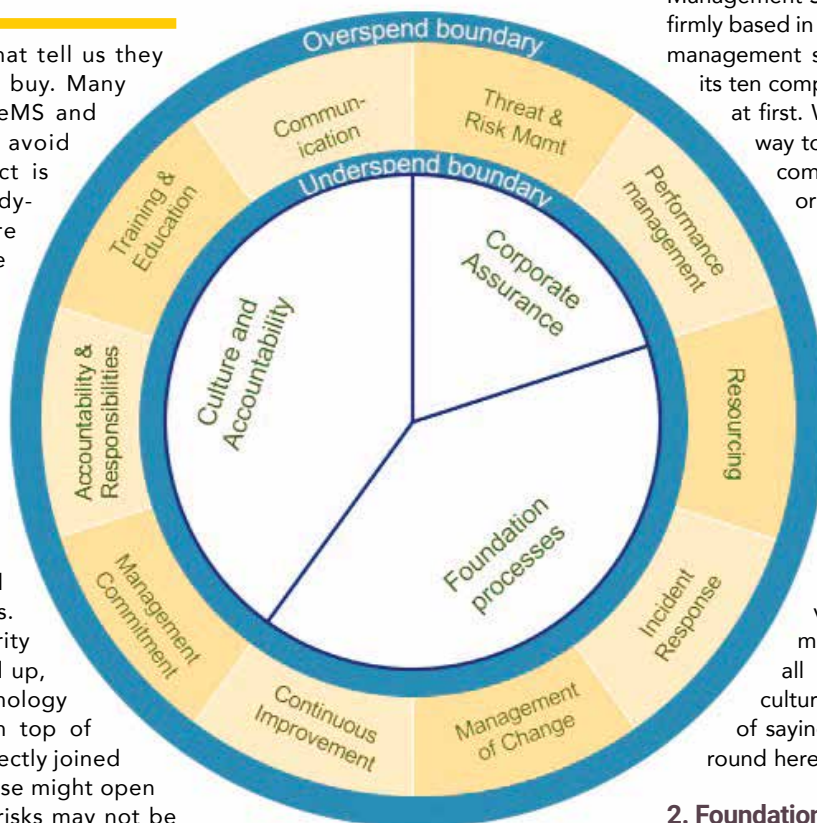
It sounds too good to be true because it is. The reality is that security is not neatly packaged up, with processes, technology and people always on top of their game and all perfectly joined up. An incident response might open other loopholes; new risks may not be spotted; decision-making may be in the wrong hands, etc.

So security is messy and the SeMS is bitty. All those loose ends to tie up; and when you go to tie them up, you find other gaps or mismatches. Multiple systems, multiple information sources, multiple fingers in the pie, some of them not even sure what they should be doing.

"...clarity of the SeMS framework can get lost – particularly ironic as the whole point of a SeMS is to give you a 'real' picture of security..."

Pity the poor security manager: no-one can see the whole picture of end-to-end security. It's a whack-a-mole task to keep risks and incidents under control, to find and close vulnerabilities, and to make sure that everyone knows what is expected of them and has the training.

The new thing the SeMS brings is the whole picture, but at first it won't be joined up. By being able to see the whole picture, security managers, accountable managers and executives can see, and fill in, the gaps one by



one. As the gaps get filled, like a jigsaw puzzle, the picture will start to be joined up.

It really shouldn't be a massive scientific or intellectual challenge; it's easy to do one edge first, and then if you have to get on with something else for a while – well, you can.

By the way, you probably have your own methodology for jigsaws; for example, join all the edges first and then work inwards. We advocate taking an equally simple approach to SeMS. Doing the puzzle builds the understanding and being involved establishes the commitment. It's unnecessary and counter-productive to buy the finished puzzle ready-made.

### So lesson number 2 is...

Building the SeMS yourself results in a SeMS you can actually use, and fosters the organisation's understanding and commitment

### Myth: SeMS needs a PhD in rocket science

'Framework for an Aviation Security Management System' is an easy read. It's firmly based in common sense and quality management systems like ISO9001, but its ten components are a lot to take in at first. We have found the easiest way to think of it is to group the components in three strands or themes:

#### 1. Culture and Accountability

A SeMS won't work without clearly defined responsibilities so people know what is expected of them, and governance that sets overall goals and accountability for delivering those goals. With leadership and the visible commitment of management to security, this all helps evolve a corporate culture, which is a fancy way of saying, "The way we do things round here".

#### 2. Foundation Processes

Once people are clear about their responsibilities, and motivated to deliver them, they need the tools to do the job. There's a whole raft of systems and procedures, some more central to security than others, but they all need to work and be easy to use – and most importantly they need to be joined up.

#### 3. Corporate Assurance

With all that in place, it becomes possible to manage the right risks correctly, and to manage the organisation's performance in delivering that.

That sounds like a lot of work but it really isn't; a lot of it will be in place already. The SeMS Framework explains clearly what each of the components

entails, and like the jigsaw, you can work at your own pace at the pieces you choose in the order that suits you best.

### So lesson number 3 is...

The SeMS model is easy to understand. It's common sense and based on quality management principles

### Myth: SeMS is just a theory with no practical value or benefits

The level of uptake from industry for what is a voluntary scheme shows the value organisations place on this framework. Without SeMS we are in the era of the flat earth. SeMS gives us a much richer, fuller and more complete picture. The earth is not flat, it's a spinning globe, and we need to see the same improvement in clarity for security. Instead of a snapshot of compliance – an inspection or management observation – which is limited in location and only known with certainty for that instant in time, the SeMS gives us a continuous picture, spots trends and gives us the assurance that we know what our security performance is.

The key areas of benefit include:

#### Continuous assurance of security

You can only address issues you can see. The board and the organisation really being able to see the security situation, managing risks and measuring security performance, is what leads ultimately to continuous assurance of security.

#### Certainty of compliance

Compliance is still as important as ever. SeMS doesn't change that but it does improve how compliance is achieved and assured. Precisely because risks are being managed and performance is measured, management has certainty of compliance, sees deviations and can fix them in good time. No surprises, no preparation needed for the inspector's visit.

"...eliminating 'abundance of caution': people appreciate they are no longer expected to do tasks they have always known were pointless..."

#### Security is improved

More certainty about security performance, and a much fuller picture of risks, not just snapshots, lead to improved security.

#### Fulfils duty of care

As custodians on behalf of the shareholders, directors have a duty of care for the security of staff, customers, the public and the business itself. The SeMS equips directors to fulfil that duty: it protects the organisation from security-related business risks, and people from harm.

#### Improved productivity

Productivity improves, with direct financial benefit. Minimising unplanned work to deal with incidents and avoiding emergency remediation work clearly reduce costs. Unplanned work is always more costly than planned, so better to be guided by the SeMS to do it right and prevent those surprises.

"...it's a whack-a-mole task to keep risks and incidents under control, to find and close vulnerabilities, and to make sure that everyone knows what is expected of them..."

#### Dispels abundance of caution

Organisations often say they are taking action from an "abundance of caution". What that usually means is, "We don't really know how secure we are". This 'Just in Case' attitude is wasteful but with greater assurance and more confidence in the organisation's security measures, it becomes possible to target resources better at where they are most needed and eliminate 'Just in Case' activities. That means lower costs for the same level of security; in other words, increased productivity.

#### Nurtures a positive culture

The SeMS nurtures an environment where security is regarded as important and everybody's responsibility, helping to generate a collaborative approach by engaging the workforce. The SeMS framework highlights the importance of this positive security culture and every component, every chapter of the framework, helps to nudge the security culture forward. One practical example is the effect of eliminating 'abundance of caution': people appreciate they are no longer expected to do tasks they have always known were pointless, which nudges the culture forward.

### So lesson number 4 is...

SeMS provides real benefits that business decision makers can understand

### Looking to the future

There is growing international take-up of SeMS in aviation, and the beginnings of its adoption in other industries. Although there are no plans yet, the UK Civil Aviation Authority anticipates that the SeMS will become mandatory. Early pioneers shaped the SeMS framework, and the current crop of implementers is continuing to shape it further.

We are already engaged in integrating SeMS with other management systems to give organisations a single unified management system in which security takes its place at the table with safety, customer service, profitability and corporate performance.

Security has made substantial advances thanks to the SeMS initiative and what will follow it will advance it further, in performance management arrangements, in the KPIs and the regulatory reporting, and in other directions not yet clear. ■

**So the last (but not least) lesson we can learn from all this is:** it's better to be involved and influencing the future of SeMS than waiting to find out what it demands.

.....  
*Andy Blackwell and John Wood are Directors of 3DAssurance.*



*Andy is widely acknowledged as a SeMS and aviation security expert. As Head of Security at Virgin Atlantic, he was the first to implement the SeMS*

*Framework. Now a leading SeMS exponent, Andy has authored numerous articles on SeMS and security, and speaks regularly at international security events.*



*John was responsible at the UK CAA for developing the SeMS framework, working with and guiding many industry stakeholders. Experienced in*

*design and implementation of effective strategic change in public and private sectors, John has been a lead designer of numerous governance, risk and compliance systems.*