

Understanding the SeMS Framework

This document is a personal record of the thinking and discussions that took place in the drafting of the SeMS Framework¹. It was produced by the leading contributors to the Framework, Andy Blackwell (previously Head of Security with Virgin Atlantic) and John Wood (previously Aviation Security Strategy Lead at the UK Civil Aviation Authority), who are now Directors of 3DAssurance Ltd.

The Framework stands on its own as a valuable and easy to read description of best practice in managing security, but we wanted to record the tacit knowledge that led to the Framework being produced – the insights and understanding, the informal discussions, the phone calls and emails, the review comments from industry and management, and the ministerial statement given in Parliament.

¹ Framework for an Aviation Security Management System (SeMS) published by the UK Civil Aviation Authority as CAP1223.

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

1. The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.
2. In order for a SeMS to be effective it should have the components described in this framework.

Why it says that

The right culture and behaviour, “the way we do things round here”, is the critical success factor for the SeMS. This commitment to doing security the right way, from the board to the front-line staff (and not only security staff), is what will make the SeMS work.

Purpose

SeMS provides a formalised, risk-driven framework for integrating security into the daily operations and culture of an Entity. The SeMS enables an Entity to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way.

“System” in the title of SeMS does not imply a software product or a piece of equipment. It is a framework for interconnecting the activities and processes that provide management control and assurance of security.

The primary purpose of a SeMS is to provide Security Assurance – to give management and staff assurance that all significant security risks are known and are being properly mitigated.

Security Assurance can only provide that certainty if the security processes and technology are *known to be* functioning properly, and if the staff and any third parties involved *understand and believe* in the importance of security, their role in it and the procedures that are to be followed.

This understanding and belief is the organisation’s Security Culture. The SeMS Framework recognizes that culture is what drives the right behaviour, and without that, the processes and tools alone cannot deliver security assurance.

To provide security assurance, the SeMS pulls together existing security activities, enhancing or supplementing them as

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

SeMS is not a mandated process but if an Entity has a SeMS which contains all the elements which are identified in this framework, it will help the Entity to meet the internal quality control provisions of articles 12, 13 and 14 of EC 300/2008².

Why it says that

described throughout the Framework, to create a formalized system of consistent and unrelenting attention to threat and risk, accompanied by the management commitment, communication and training to lead the organisation's security culture.

There is no requirement in the regulations for an organization to have a SeMS. However there are quality control requirements in Articles 12, 13 and 14, but these are not spelled out in any detail. A second purpose of a SeMS is to provide those quality controls.

There is a third purpose not explicitly stated in the Framework. Not only is having a SeMS voluntary, that SeMS does not have to match the Framework. However, the CAA hopes in time to be able to use SeMS outputs as a major source of oversight data. This will be immensely helpful to regulated organisations because it will ensure the CAA gets a clear picture of consistent performance rather than the snapshots afforded by the observation and inspection regime. It mitigates the risk of the CAA catching staff on a bad day and that poor performance becoming the CAA's assessment of the organization as a whole.

For the CAA to be able to interpret the data it receives, there will have to be considerable commonality of what organisations' SeMS provide. Without that, the organisation's data may be misinterpreted or ignored, so it makes sense for an organisation to design its SeMS to match the Framework wherever possible.

² Regulation (EC) 300/2008 of the European Parliament and of the Council of 11 March 2008.

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

Why it says that

There has been general agreement in industry that the Framework is well-judged, clear and not too prescriptive, and it is SeMSnet's view that properly thought-out adoption of the Framework will yield all the benefits without creating a bureaucratic burden.

Implementation

A SeMS Manual need not be a separate document. Many of the components will already exist in an Entity's security programme, operational processes, operating procedures or other documents. In order to have a security management system, an Entity only needs to include in its SeMS Manual an index or map of its existing documents, systems and records provided the latter meet the requirements of this Framework.

Depending on its size and complexity, an Entity may decide to combine its security policy, security programme and SeMS Manual into a single document or to keep them separate as complementary documents.

Whatever form the SeMS Manual may take the SeMS itself should be part of the Entity's overall management system.

The Framework is seeking to guide organisations to improve rather than replace or duplicate their security management arrangements. Organisations do know how to manage security: they are doing it already and there is no need, in fact it would usually be counter-productive, to duplicate existing processes. However the Framework does suggest one new document – the index or map - which would help staff and regulators alike understand how the SeMS works.

The SeMS is itself a management system. For security to gain its deserved status at board level, the Security Management System must be accorded the same importance as the systems for other aspects of the business such as safety management, financial management, quality management, business risk management and customer service management.

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

Why it says that

There is a view gaining momentum that these systems will ultimately combine into one integrated management system, but in the meantime SeMS outputs must be part of management decision-making along with the other aspects.

SeMS philosophy

The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.

In order for a SeMS to be effective (for both industry and the CAA) it should include the components set out in this document.

The Framework describes the 10 components Chapter by Chapter, but the mechanical processes and tools are not enough. The whole organization, its management, staff, partners and suppliers must buy into the importance of managing security and the value of managing it the SeMS way. Only then will the Framework be regarded as a helpful guide to a good SeMS. Otherwise it is merely a set of requirements which will get varying degrees of acceptance from staff.

The spoked wheel diagram in the Framework illustrates how this Culture is the hub enabling all the components to connect and work together.

“Culture” is a much used and abused term. In the SeMS context it means (approximately!) a belief in, and buy-in, to the concept of SeMS, an understanding of the behaviours needed to support the SeMS, and a willingness to adopt those behaviours. The culture becomes fully embedded when those behaviours have become instinctive.

Perhaps a better way to describe culture is “It’s the way we do things round here”.

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

Key components of a SeMS

A SeMS should include the following components, applicable to all types and sizes of Aviation Entity:

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. SeMS education and security culture
10. Communication

Chapters 1 to 10 cover each of these components in turn.

Note that the SeMS Framework includes Confidential reporting in Chapter 5 – Performance monitoring, assessment and reporting. In the 3DAssurance model, we treat it as a separate component, #11.

Why it says that

These components fulfil three key themes of security management:

Theme	Chapter
Corporate Assurance The tools for managing security risks	2. Threat and risk management 5. Performance monitoring, assessment and reporting & Confidential reporting 6. Incident response
Culture & Accountability Mechanisms for explaining what is expected of people and motivating them	1. Management commitment 3. Accountability and responsibilities 9. SeMS education and security culture 10. Communication
Enabling processes Four of the key processes that enable the SeMS to operate effectively	4. Resources 7. Management of change 8. Continuous improvement

Key Points

Understanding the SeMS Framework

Introduction

What the SeMS Framework says

1. Treat SeMS as a project and ensure governance and resource is allocated to see it through.
2. There is no need to recast existing documents, procedures, etc. if they support a SeMS. The brigading of security material into one manual has advantages, provided clear cross-referencing is applied.
3. The creation of an embedded security culture, akin to that for safety, is a core driver for a SeMS.
4. Collection, analysis and use of honest and accurate data is essential.

Why it says that

The first three of these are advice on the creation of the SeMS. The fourth is a key requirement of the SeMS in operation

Chapter 1 – Management Commitment

What the SeMS Framework says

The Entity's management should show its commitment to security by:

1. **Board-level and senior management support of the SeMS**
2. **Promoting a positive security culture**
3. **Key appointments that reflect the importance of the SeMS**
4. **Determining and providing the appropriate resources**

Why it says that

Leadership and visible moral commitment from the top, “walking the walk” not just talking the talk, is the first key requirement.

This must be underpinned by practical commitment in the form of senior appointments responsible for security and the SeMS, and properly considered assessment of resource needs. These two practical requirements are covered in Chapters 3 and 4 respectively.

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

Why it says that

Senior management commitment

Senior management should:

- promote the Entity’s security policy to all personnel and demonstrate their commitment to it;
- establish the Entity’s security objectives and performance standards; and
- determine and provide the necessary human and financial resources for the SeMS.

The committed and visible involvement of senior management is critical to an effective SeMS – one that provides the security assurance. Top management must lead the implementation and ongoing use of SeMS, giving the cultural leadership by demonstrating belief and buy-in. They must also give the practical leadership by directing the organisation on what SeMS is and is not; explaining their objectives for SeMS; and making – and explaining – the decisions on priorities and resourcing. Commitment to SeMS does not demand unlimited resourcing, but it does demand resourcing decisions that take into account the management view of risks, priorities and objectives. If staff can see the rationale, they will believe the commitment.

All of this explaining, demonstrating and leadership is wholly dependent on excellent communication. Because of its importance, communication has its own chapter (chapter 10) in the Framework.

Security policy statement

The security policy is the means whereby the Entity states its intention to maintain and, where practicable, improve security levels in all its activities.

The security policy is senior management’s shop window for its intentions about SeMS. It is the means of demonstrating that the commitment to SeMS is consistent from the Board down and that security is treated at Board level with appropriate dedication, purpose and resolve. The communication of the security policy and

The security policy should:

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

- be endorsed by the Accountable Manager;
 - identify security as a high organisational priority mutually supportive of commercial and operational priorities;
 - reflect organisational commitments regarding security and the Entity's proactive and systematic management;
 - be communicated throughout the Entity;
 - include security reporting principles;
-
- be periodically reviewed to ensure it remains relevant and appropriate to the Entity;
-
- include a commitment to:
 - a) a continuous improvement programme;

 - b) ensure Aviation Security Requirements and all applicable standards are met, and consider best practices;

Why it says that

The bullet list describes how the security policy should be used to make the management commitment visible to staff and what the security policy should include.

- Visibility of management commitment.
- Positions security alongside and equal to considerations such as customer service, finances and health and safety.
- Explains how the positioning of security (previous bullet) is actually implemented – and is not just words.
- Reinforces visibility of management commitment – note that communication should be repeated creatively.
- Explaining that security performance is to be measured and reported demonstrates that management is serious about SeMS.
- An unrefreshed security policy is a message that management no longer sees security as a priority. Even if no changes are required, re-issue of the security policy shows management is still committed, and communicating the updated policy is an opportunity to reinforce the security culture.
- This is the core content of the security policy.
 - a) Continuous improvement is central to SeMS. Having a fixed target for security performance is counter to the SeMS philosophy and organisations should be doing whatever the risk assessment determines is needed. – and that will change as circumstances and capabilities change. Chapter 8 discusses this in more detail.

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

- c) provide appropriate resources;
- d) enforce security as the responsibility of all personnel;
- include security reporting procedures (including access to the Anti-Terrorist hotline) and whistleblowing arrangements; and
- promote a positive security culture.

Why it says that

- b) Because the regulations have been the way of life in security, any hint that SeMS ignores them will only discredit SeMS. It is important to state clearly that SeMS is not replacing them.
- c) Providing the required resources is a pre-requisite of a successful SeMS. It is also a clear demonstration of management commitment.
- d) Making security the responsibility of the whole organization (and its third parties) is the key cultural shift needed to make SeMS the organisation's management system, and not just a tool for the security specialists. The security policy alone will not achieve this, but should explain the actions that management is taking to achieve it.
- This bullet refers to the reporting of security 'occurrences'. These may be full-blown incidents, but they may also be smaller issues, worries or observations. If all staff are to be responsible, they must have a means to act, which for many of those not directly involved in security procedures will be to report the issue for management to take action. This can be a powerful cultural tool. On the positive side, it demonstrates that management is expecting all staff to take responsibility. On the negative side, if management is not seen to act on the reports it is a strong signal that management is not serious about SeMS or security.

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

Why it says that

→ An explicit commitment to promote the right security culture is important as a demonstration of management commitment to improve how the organization treats security through the SeMS. However it must be followed up by overt promotional actions to avoid being seen as an empty promise. Many of the other bullets provide opportunities for promotion and these should be exploited energetically.

Key appointments

The Entity's management should ensure the following key roles are filled with suitably qualified and skilled individuals.

SeMS depends on two key roles being fulfilled: the Accountable Manager to provide Board level sponsorship and leadership; and the Security Manager to provide the deep security assurance and SeMS expertise.

Accountable Manager

The Accountable Manager's role is to instil security as a core organisational value and to ensure that the SeMS is properly implemented and maintained through the allocation of resources and tasks.

The Accountable Manager is the champion of SeMS. (S)he has the classic sponsoring role described in Prince2, MSP and MoR. All those methodologies give useful insight into the responsibilities, relationships and skills of the role.

The Accountable Manager may have more than one function in the Entity but should have sufficient authority to be able to direct both finance and resource to the security operation.

The Accountable Manager is not a full time role. Ideally the role will be assigned to someone who already has a senior responsibility for security, quite likely along with other duties.

The Accountable Manager should be the Chief Executive Officer (CEO) of the Entity or a suitably competent and qualified person appointed by the CEO, taking into account the size, structure and complexity of the Entity.

This shows the importance the Framework puts on the level of discretion and authority the Accountable Manager has. The Accountable Manager must have sufficient power within the organization to fulfil the sponsoring role properly.

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

The Accountable Manager should have a thorough knowledge and understanding of the key issues of risk management within the Entity.

The Accountable Manager's technical knowledge and understanding of SeMS should be sufficient to perform the Accountable Manager role. The Accountable Manager need not know about all the detail of security processes within the Entity but should have an understanding of how the Entity's assurance of the regime is maintained.

Depending on the size and complexity of operations, the Accountable Manager may delegate specified tasks. However, accountability and responsibility for those tasks remains with the Accountable Manager.

More details on the **role** of the Accountable Manager can be found within CAP1224 – Guidance Notes for Accountable Managers (<https://www.caa.co.uk/cap1224>)

Security Manager

The Security Manager should be the focal point for SeMS and should be tasked with managing the development, administration and maintenance of an effective Security Management System.

The Security Manager should:

Why it says that

Sponsoring SeMS requires a real understanding of risk management rather than detailed knowledge of the security regulations.

Tasks can be delegated; accountability cannot. The sponsor remains responsible for facilitating the success of SeMS and delegating the role of 'Being the sponsor' will tell staff that the organization's management is not committed to SeMS.

Correct title CAP1224 – Security Management Systems: A guidance note for Accountable Managers

Security Manager

The SeMS provides new 'tools' for security management. The SeMS complements the existing tools so the primary SeMS user is the person already responsible for security assurance – the Security Manager – who can be regarded as the SeMS controller.

These bullets highlight key SeMS-related responsibilities, but many of these may already be in the Security Manager's pre-SeMS job description. The SeMS builds on existing security

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

- facilitate threat identification, risk analysis, and management;
- monitor the implementation and functioning of the security management system, including any security actions that the Entity considers necessary;
- manage the security reporting system of the Entity;
- provide periodic assurance reports on security performance to the Entity's Accountable Manager and Board;
- ensure maintenance of security management documentation;
- ensure that security management training that the Entity considers necessary to implement its security operation and its SeMS, is available;
- provide advice on security matters to the Entity; and
- participate in internal occurrence/security investigations.

The Security Manager should have:

- practical experience of and expertise in the Entity's operations;
- knowledge of security and quality management;
- knowledge of the Entity's security programme; and
- comprehensive knowledge of the Aviation Security Requirements applicable to the Entity.

The Security Manager may be any suitably competent and qualified person at appropriate management level, provided that that person can act independently of other managers within the Entity, and has direct access to the Accountable Manager and to appropriate management personnel to raise security matters.

Why it says that

arrangements and while the SeMS may extend or bring extra intensity to them, the Framework aims not to duplicate anything.

Likewise the Security Manager's expertise requirements are not specific to SeMS. Clearly the SeMS controller should have the requisite security expertise and knowledge but the SeMS requires little in the way of new SeMS-specific skills. Like the processes though, the depth and intensity of the expertise required may be increased.

The Framework avoids being prescriptive about the Security Manager's position within the organization but it does require that the controller of the SeMS has the organizational freedom and management access to do the job effectively.

Understanding the SeMS Framework

Chapter 1 – Management Commitment

What the SeMS Framework says

Key points

1. It is vital that senior management commit to SeMS at the outset and provide sustained support to the process as it is developed.
2. Ensure that adequate and appropriately skilled resource is provided for SeMS development and, wherever possible, that this resource is not diverted to other tasks.
3. The Security Policy should be focussed, rooted in SeMS principles, visible and shared with staff so that it becomes ingrained in the culture.

Why it says that

The SeMS will change the culture of the organisation and establish security as a core strategic activity. Without committed management is a critical factor for success.

Although not expensive, SeMS does requires some resources and, preferably, dedicated resources.

The Security Policy is another critical success factor. It is the manifesto that puts security on the top management agenda, and makes its importance clear to staff.

Chapter 2 – Threat and risk management

What the SeMS Framework says

A SeMS should provide:

1. A process for identifying local threats
2. A threat assessment and scoring process
3. A process for assessing the security risks
4. A review process to identify, and monitor the effectiveness of, the mitigations for those risks

Why it says that

Effective threat and risk management is the core product of the SeMS. Other chapters deal with the mechanisms that enable Threat and risk management to work and monitor its effectiveness.

Local threat identification process

Understanding the SeMS Framework

Chapter 2 – Threat and risk management

What the SeMS Framework says

National and international threats are notified to the Entity by the Government and mitigated by regulatory measures. The Entity's threat identification process should supplement this information with a list of locally-identified threats suitably defined and assessed for subsequent use in risk assessment.

When conducting risk and threat assessments Entities are encouraged, where appropriate, to adopt a multi-agency approach as airports currently do. For further information please see the guidance referenced below:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/11516/guide.pdf

Why it says that

Consistent and unrelenting attention to threat and risk is the primary goal of effective security management. The SeMS depends on an organisation searching out its own threats, including variants of the 'national' threats, and putting this information at the centre of its security management approach.

Airports already conduct a multi-agency approach to threat identification and risk assessment and the Framework encourages all organisations to adopt similar thinking.

This link is incorrect. The correct link is

<https://www.gov.uk/government/publications/airport-security-planning-quick-guide>

Assessing vulnerabilities

The threat and risk assessment process should capture a clear and comprehensive picture of where vulnerabilities exist. Only by establishing where vulnerabilities lie can adequate mitigation be considered and assessed.

A threat only poses a risk if there is a vulnerability that would enable the threat to materialize. Understanding the vulnerabilities is a prerequisite of correctly prioritizing the threats and the risks they pose. Mitigations are not needed for threats that cannot materialise, but that principle must be used with caution – before deciding against mitigation, it is necessary to be absolutely certain that the threat cannot materialise.

Assessing risks

Understanding the SeMS Framework

Chapter 2 – Threat and risk management

What the SeMS Framework says

Following assessment of each vulnerability and threat faced by the Entity, the actual risk of such an event occurring and succeeding should be assessed by the Entity.

Security risk assessment is the analysis of the security risks that have been determined.

Security risk analysis breaks down the risks into two components – the probability of occurrence of a damaging event or condition and the severity of the event or condition, should it occur. Security risk decision making and acceptance should be specified by the Entity through a risk tolerability matrix.

Why it says that

In this section the Framework outlines the typical stages of a risk assessment process.

The highlights of risk management, including risk assessment, are described in the SeMSnet document 'Risk Management Primer'.

Risk analysis, probability, severity and tolerability are also covered by the Risk Management Primer and the government-sponsored Management of Risk approach also provides a useful in-depth description of risk management.

Review process

The risk register and the mitigations arising from it should be reviewed by the Entity on a regular basis and as and when the threat situation changes.

A formal security risk assessment and mitigation process should be developed and maintained by the Entity that ensures analysis (in terms of probability and severity of occurrence), assessment (in terms of tolerability) and control (in terms of mitigation) of risks.

The frequency of review should depend on local context such as the size or complexity of the operation.

Whilst the risk register is the repository of all risk information, it is only of value if it is regularly used to drive every element of the risk management process, from analysis to mitigation.

This paragraph outlines what the risk management process must achieve. Again, the Risk Management Primer and the Management of Risk approach provide useful guidance.

Key points

Understanding the SeMS Framework

Chapter 2 – Threat and risk management

What the SeMS Framework says

1. Local liaison is important. Sharing of information with partner entities is encouraged. This will achieve a more comprehensive local threat picture than acting alone, will reduce duplication of effort and enable joined-up threat mitigation.
2. Local police are a source of up to date local crime information.
3. As much as is possible, share information with your people – involve them in acting as your eyes and ears.

Why it says that

Information sharing is common in safety management – sharing within the business, sharing with partners and authorities, and to some extent sharing across the industry. Security, by its nature, tends to be secretive and this secrecy tends to be applied indiscriminately to all aspects. Sharing with partners may not therefore happen naturally and should be made to happen.

Local police and the organisation's own staff are also partners in delivering and managing security. Information sharing with them is equally or more important.

Chapter 3 – Accountability and responsibility

What the SeMS Framework says

The SeMS should include:

1. **Clearly defined accountability and responsibility for security throughout the Entity**
2. **Clearly defined governance arrangements that ensure security is accorded sufficient priority and management attention**

Why it says that

People must be clear what is expected of them, and be provided with a governance framework within which to operate. This is similar to other accountability and governance in the company, such as financial control, or decision-making authority.

Defined accountability and responsibilities

Understanding the SeMS Framework

Chapter 3 – Accountability and responsibility

What the SeMS Framework says

The Entity should define accountability and responsibilities for security throughout the Entity, including security governance responsibilities at all levels.

Why it says that

This chapter builds on the Management Commitment (Chapter 1), which defines accountabilities and responsibilities for the Accountable Manager and Security Manager.

Chapter 1 makes it clear that (almost) all staff have a security responsibility. Whilst the Management Commitment is a key element of the leadership of SeMS, staff throughout the organization do need to know their responsibilities, role by role. Every role description should consider what security accountability and/or responsibilities need to be specified.

Security governance mechanisms

The Accountable Manager should put in place governance arrangements that provide the Entity's management with assurance that security processes are effective and that the SeMS is fit for purpose.

The governance mechanism should consider matters of strategic security in support of the Accountable Manager's security accountability. It should:

- monitor security performance against the Entity's security policy and objectives;
- monitor the effectiveness of the Entity's operational security and its security management processes;
- in order to monitor performance against objectives, those objectives must be set at high management level
- effectiveness is measured by assessing the performance levels against the levels defined or implied by objectives

Understanding the SeMS Framework

Chapter 3 – Accountability and responsibility

What the SeMS Framework says

- ensure that data is an honest and accurate reflection of performance;
- monitor the effectiveness of the Entity’s operational security and its security management processes;
- ensure that any security action is taken in a timely manner; and
- ensure that appropriate resources are allocated to achieve the Entity’s intended security performance.

Depending on the size of the Entity and the type and complexity of its operations, existing governance structures may be extended to incorporate these governance responsibilities. For example, airports maintain a multi-agency Security Executive Group (SEG)² and Risk Advisory Group (RAG)³, which, with regard to airports, could fulfil the governance responsibilities described⁴.

Other Entities are encouraged to adopt a similar approach where appropriate.

Why it says that

- unless the information is reliable, decision –making will be compromised
- {this bullet has been duplicated in the Framework in error}
- performance reporting is periodic: more immediate monitoring is also needed that planned actions are taken at the planned time
- although some budget responsibility may be delegated, the board has ultimate control of the resources allocated to all operations. Resourcing of security must be given the same consideration as other activities at board level.

Here and throughout, the Framework encourages use of existing processes and structures wherever possible. It gives the example for airports of the SEG and RAG and their roles in governance and suggests that it could be used as a model by other organisations.

Footnotes

² The Security Executive Group (SEG) brings together people who have the authority to take decisions about the security measures that should be put in place. It includes

Understanding the SeMS Framework

Chapter 3 – Accountability and responsibility

Why it says that

What the SeMS Framework says

senior representatives from the airport operator, the local police force, the local police authority and airlines operating at the airport.

3 A Risk Advisory Group (RAG) brings together security practitioners at the airport, including representatives of the airport manager and local chief officer of police. The RAG's function is to produce a Risk Report, assessing each threat to the security of the airport. The RAG then makes recommendations about the security measures that should be taken, or continue to be taken.

4 Guidance on SEG and RAG can be found at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/11516/guide.pdf

This link is incorrect. The correct link is
<https://www.gov.uk/government/publications/airport-security-planning-quick-guide>

Key points

1. Clear accountability and terms of reference bring dividends.
2. Regular and effective monitoring of performance, with accurate and meaningful data is essential for good governance.
3. Use existing structures where appropriate.
4. **A simple diagram can aid communication and understanding of the governance structure.**

The first two points are critical success factors.

The last two are advice learned from observing organisations implementing a SeMS.

Understanding the SeMS Framework

Chapter 4 – Resources

What the SeMS Framework says

An effective SeMS depends on:

1. Provision of adequate resources, facilities, equipment and support
2. The Entity placing an appropriate degree of importance on security in the selection of personnel
3. Appropriate specifications for security equipment and services and maintenance
4. Effective contracting and oversight of 3rd parties, contractors and suppliers

Why it says that

However clear staff may be about their responsibilities, and however motivated they may be, they cannot fulfil their roles effectively if they do not have adequate resources. This includes the quantity and quality of personnel, the quality of the working environment and the availability of suitable equipment and services needed for the job.

Provision of resources, facilities, equipment and supporting services

The Entity should determine and provide the appropriate resources that it needs to:

- implement and maintain the SeMS; and
- implement and maintain the security processes that deliver the SeMS, the Aviation Security Requirements and any other risk mitigation identified.

Personnel contributing to a security process should be competent and have appropriate education, training, skills and experience.

In most organisations, budget limits constrain all activities. The Framework does not expect unlimited resources to be allocated to SeMS and to security generally, but it does expect the organisation's management to make informed decisions on resourcing, taking into account the risk picture and current security performance. Whatever resourcing management decides upon, it should do so in full knowledge of the impact of that decision on risk and performance.

Personnel – staff, contractors and third party suppliers' staff – are one of the key resources that should be determined by

Understanding the SeMS Framework

Chapter 4 – Resources

What the SeMS Framework says

The facilities, equipment and supporting services provided should be sufficient, suitable and maintained to achieve the security outcomes, including the Aviation Security Requirements.

The Entity should keep records of these resources for security management and performance reporting purposes, as defined in its SeMS.

Why it says that

management. This includes quality as well as quantity – skills, experience and education.

The other key resources are the physical assets and supporting services, and as for personnel the quality is as important as quantity. This will be seen again below in relation to supplier performance.

Records need to be kept to enable management to assess historically the impact of their resourcing decisions on performance, and also to facilitate internal and regulator audits.

Personnel competences for the SeMS

The Entity should provide adequate resources for planned tasks by:

- determining the required competences and qualifications for each role;
- stressing, for appointments to senior roles, the importance the Entity places on security; and
- providing suitably qualified personnel.

This section explains the considerations the Framework expects management to apply to the selection of personnel to fulfil the resourcing decisions. In summary, a SeMS resource requirement should not be regarded as fulfilled until it is confirmed that the assigned personnel are of the right quality.

Management of third party suppliers

The ultimate security responsibility for any product or service provided to the Entity by contracted entities remains with the Entity.

Many organisations will outsource some aspects of their activities, including activities directly or indirectly affecting security. Legally the ultimate accountability if those activities are sub-standard lies with the organization, and it cannot simply blame the third party supplier.

Understanding the SeMS Framework

Chapter 4 – Resources

What the SeMS Framework says

The Entity should define responsibilities within its own organisation for managing contracted security activities, including quality assurance of what the 3rd party is providing.

The contracted activities should be included in the Entity's SeMS.

Why it says that

The security performance (along with other aspects of performance) of the third parties must be managed by the organization, and the impact of that performance on the organisation's security must be managed through the SeMS

Receiving third party services

Where the Entity is receiving a 3rd party service which impacts aviation security, it should, where appropriate, specify in the SeMS any security-related requirements, including the provision of information by the 3rd party, to enable the Entity to assure security performance.

In order to manage third party security performance, the organization must first specify the performance it requires from the third party. This should include auditable data and reports from the third party about its performance.

Providing third party services

Where the Entity is providing a security-related service to another Entity which could affect aviation security, information should, where possible, be shared with that Entity to provide assurance of security performance.

An organization committed to SeMS principles should willingly provide data and reports about its own performance as a third party to enable its customer to manage its security performance.

Key points

1. Wherever possible, maintain consistent SeMS resource in order to develop expertise and maintain consistency.
2. Senior managers should lead in delivery of the SeMS security culture.

Personnel (staff, contractors and third party suppliers' staff) , physical assets and supporting services are key resources that should be determined and managed. This includes quality as well as quantity – skills, experience and education of personnel,

Understanding the SeMS Framework

Chapter 4 – Resources

What the SeMS Framework says

3. 3rd party providers should be part of the SeMS as well as being managed by it.
4. The heart of a SeMS is the sharing of information and data - delivering a collaborative SeMS.

Why it says that

quality and reliability of equipment, consistency of service from 3rd parties.

Resource quality can only be assessed if the required information on performance is provided by the 3rd party.

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

The SeMS should include:

1. What performance measures are used
2. How data is analysed to improve security
3. How security performance is reported internally by the Entity
4. How data is stored and protected by the Entity

Why it says that

Chapter 2 described the approach to Threat and risk management and its core role in the SeMS. The effectiveness of Threat and risk management was identified as a key issue to be reviewed and the outcomes of the risk management activity are a key focus for the Performance monitoring.

Security performance does include compliance performance but this should be seen as just one element of how well the organisation is managing its overall security and risk exposure. In fact, compliance with regulations is itself a risk mitigation measure, since the regs are designed to deal with predefined risks.

Performance monitoring and measurement process

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

The Entity should use performance monitoring and measurement to verify its performance of the security processes against the Aviation Security Requirements and the Entity's security policy, objectives, identified risks and specified mitigation measures as defined in the SeMS.

This process should include the setting of security performance indicators and security performance targets and measuring the security performance against them.

All levels of relevant management in the Entity should have oversight of key performance indicators.

The performance monitoring and measurement process should include:

- addressing the performance in relation to the Aviation Security Requirements;
- assessing how effective a security process is and not just checking if it is taking place;
- security reviews including trends reviews which are conducted during introduction and deployment of new technologies, change or implementation of procedures, or in situations of structural change, or to explore an increase in incidents or security reports;
- security audits which focus on the integrity of the management system;

Why it says that

Having determined what security processes to operate, including mitigations for the risks it has identified, the organization needs to know how effectively it is carrying out those processes and mitigating the risks.

Security performance indicators, like a speedometer, give a good picture of performance and can be used for assessing performance over time as well as the performance at a point in time. Performance targets, like a speed limit, set goals for the performance indicators.

Different managers may have different information, needs for and/or they may need measurement to be made over different time periods.

These bullets summarise the main types of measurement likely to be required.

- Performance in terms of the degree of compliance with the regulations
- “How effective is our security?” is the key assurance question and measurement should be designed to answer this;
- Periodic reviews, and comparison of those results with past periods in a variety of situations: steady state (no changes); changes to operational or security technology or the premises; changes to operational or security procedures; organizational changes; changes in performance levels
- It is important to confirm that the SeMS is working properly if it is being relied upon for security assurance

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

- examination of particular elements or procedures of a specific operation; and
- internal security investigations of security incidents.

Why it says that

- Performance reports, trends or audits may identify areas needing examination
- Incidents are a potential source of information about security performance generally or in specific areas

Analysis of data

The Entity should determine, collect and analyse appropriate data to demonstrate the suitability of security processes and to evaluate where improvement of the effectiveness of the security processes can be made. This should include data generated as a result of monitoring and measurement and may include data from external sources.

Data in this context includes performance measurements but also any other sources of information, including externally-produced data, whether from third parties, the regulator, or public sources. The goal is to find indicators not only of performance of the processes, but also of the suitability and effectiveness of those processes. This paragraph encourages organisations to search for data and then to use it to analyse it and evaluate the processes.

Corrective action

The Entity should take action to eliminate the cause of poor performance in order to prevent recurrence.

Any corrective actions should be appropriate to deal with the effects of the poor performance identified by the Entity.

A documented procedure should be established to define requirements for:

- reviewing poor performance;

The next two sections deal with corrective actions (putting right failures) and preventive actions (stopping failures occurring).

The corrective actions must repair the damage caused by the failure. It should not be assumed that it is sufficient just to redo the failed action correctly.

The bullets describe the components of the corrective action procedure, namely:

- investigate what happened
- identify what caused it

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

- determining the causes of poor performance;
- evaluating the need for action to ensure that poor performance does not recur;
- determining and implementing the appropriate action; and
- reviewing corrective action taken.

Why it says that

- determine whether preventive action is also required (see next section for preventive action)
- identify the rectification needed to eliminate the failure and repair the damage
- conduct a review of the corrective action to ensure it had the intended corrective effect

Preventive action

The Entity should determine action to eliminate the causes of potential poor performance in order to prevent their occurrence. Preventive actions should be proportionate to the effects of the potential poor performance.

A documented procedure should be established to:

- determine potential poor performance and its causes;
- evaluate the need for action to prevent occurrence of poor performance;
- determine and implement the appropriate action; and review preventive action taken.

Preventive action will almost invariably follow corrective actions. When a failure occurs, it is first repaired (corrective action) and then appropriate steps taken to prevent the failure occurring again. The Framework points out the need for proportionality: minor failures may not justify major investment in prevention.

The bullets describe the components of the preventive action procedure, namely:

- identify where problems may occur and the causes; in the case of failures that have already had corrective actions this is straightforward but there may also be potential problems that have not yet occurred and which need prevention
- assess whether preventive action is needed, taking into account the severity of the actual or potential failure
- determine what preventive action could be taken, and whether the severity of the actual or potential failure justifies it; record actions taken (including any decision not to take

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

Why it says that

action); review the effectiveness of the preventive actions after they have had time to take effect

Management of security data and information

The security management objective for management of data and information should be to ensure the security of data and information received and used so that it is protected from interference, and access to it is restricted only to those authorised.

This paragraph applies to all data but especially to performance data. Any information that is relied upon for security assurance must be dependable and therefore must be protected from being changed, deleted or lost.

Security reporting system

The overall purpose of the security reporting system is to use reported information to improve the level of security performance and not to attribute blame.

This section describes the security and confidential reporting system which is used for reporting and recording incidents and other security occurrences (events that are less than incidents but still significant). The first paragraph is a reminder that reports are for managing and improving security, not attributing blame.

The objectives of the security reporting system should be to:

- enable an assessment to be made of the security implications of each relevant occurrence or serious incident, including previous similar events, so that any appropriate action can be initiated; and
- ensure that knowledge of relevant occurrences and serious incidents is disseminated both internally and externally,

The bullets describe the objectives of the reporting system:

- assessing the security implications of occurrences and incidents. Note that incidents may have been managed through the Incident management process (Chapter 6) but the reporting system may be how it is first reported and/or how its impact is managed once the incident itself has been dealt with

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

where appropriate, so that others may learn from them and adapt behaviours accordingly.

The security reporting system should have the capability to confirm receipt to the reporter, where appropriate.

The reporting process should be simple and clearly defined including details as to what, how, where, to whom and when to report.

Regardless of the source or method of reporting, once the information is received, it should be stored in a manner suitable for easy retrieval and analysis.

Access to the submitted reports should be restricted to protect the identity of the source, where appropriate.

The security reporting system should include a feedback system to the reporting person on the outcome of the occurrence analysis.

Why it says that

- having procedures or tools to share across the organisation the knowledge gathered by the reporting system and the lessons learnt

If the system is not actually accessed by the reporter (for example if events are entered into the system by a call centre), it should send him/her a confirmation that the event has been recorded.

Users will need guidance on what kind of events to report. To ensure events are reported it is likely to be necessary to make reporting of certain incidents and occurrences mandatory.

Users will not use the system frequently enough to become familiar with it. The system must be easy to use with clear guidance or users will be unwilling to use it.

The incident and occurrence data must be capable of being accessed by authorised analysts (subject to appropriate access controls) to enable meaningful analysis.

Tight control of access to this information is important simply because it relates to security weaknesses. In addition the source of a report should not be readily identifiable, even to the authorised analysts. The access controls must be sufficiently refined to protect the anonymity of the reporter whilst still feeding back outcomes.

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

The security reporting system should also include a voluntary confidential reporting process for reporting security matters. An Entity’s existing “Whistleblower” reporting process may be suitable for this.

Why it says that

The system should facilitate feedback but there may be circumstances where it is not appropriate to feedback any further than to say the report has been dealt with.

The focus of this paragraph is the promotion within the organization of voluntary reporting in addition to the mandatory reporting of incidents and occurrences.

The purpose of voluntary confidential reporting is that it encourages honest reporting of mistakes (but also allows malicious reports). The access controls discussed earlier in this section would be adequate to protect voluntary reporters.

Record keeping

The system used by the Entity for record keeping should provide adequate procedures for storage and backup. The system should ensure records are traceable, retrievable and accessible by those authorised.

The system should include safeguards to ensure the confidentiality, integrity and availability of the information is maintained.

All security data, including performance and incident/occurrence reports, must be secured. The information must be readily accessible (by appropriately authorized people) when needed and not at risk of loss or damage. It must also be traceable – i.e. the context, date, location, version and similar characteristics must be clearly identified so there is no doubt what situation the data relates to.

Quality assurance of data and information

Honest and accurate data is essential for a SeMS to work and for Board and Regulator assurance. The quality of security-related data and information should be assured by a quality

The previous section dealt with storage and protection of security data. This section adds the requirement to assure the

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

management system that controls the origination, production, storage, handling, processing, transfer and distribution of that data and information.

Why it says that

quality of that data. There is no point in safe storage and backup of information that is incorrect.

The purpose of the quality management system is to ensure the data is captured accurately and not corrupted as it is handled by the various procedures and systems it is processed and held in.

The original Framework principles apply here.

It is not the intention that the organization should build a comprehensive quality management system just for the purpose of assuring the security data. The organization may already have a quality management system which can be used for this purpose, or the necessary quality management may be implemented relatively simply within the SeMS. It may take the form of a few control procedures or it may only require a few controls added to existing procedures.

Key points

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. Collection, analysis and sharing of honest and accurate data is an essential SeMS principle. 2. Effective, targeted performance measurement and reporting is part of the bedrock of a SeMS. 3. Think wider than security requirements - how can overall performance be improved and potential gaps closed? | <p>Without accurate data, performance monitoring is worthless, but many of the data sources will be subjective, making honesty and avoiding self-delusion paramount.</p> <p>“Measure the right things and measure them right” is a mantra for effective performance monitoring.</p> <p>If security is to be truly risk-based, its performance must include its ability to deal with unknowns, not just compliance or meeting defined requirements.</p> |
|---|--|

Understanding the SeMS Framework

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says

4. An open SeMS is a good SeMS. Clear reporting procedures will encourage involvement.

Why it says that

Reporting performance should be a major driver of culture. It's not about catching people doing things wrong, it's about demonstrating that they're doing a lot of things right.

Chapter 6 – Incident response

What the SeMS Framework says

The SeMS should include:

1. A security incident response process
2. Methods of testing, reviewing and improving the response plan
3. A procedure for the introduction of additional security measures

Why it says that

Incidents change the 'steady state' operational environment for which security procedures and risk mitigations have been designed.

The response to incidents must not only deal with the incident, but also assess whether security has been compromised, either by the incident or by the response actions, and must then deal with any such compromises. If temporary measures are introduced, the response plan must ensure security is not compromised when they are discontinued after the incident.

In order to ensure the constant readiness of the response plan testing and reviewing should be put in place. Finally, the response plan is not static, it will be changed when other operations change, but also opportunities to improve it should be sought during the testing and reviews.

Incident response

Understanding the SeMS Framework

Chapter 6 – Incident response

What the SeMS Framework says

All SeMS should include response processes for dealing with security incidents. The processes should be exercised or reviewed as appropriate on a regular basis.

Why it says that

The Framework gives little guidance on the incident response process itself, since all organisations will have procedures for managing incidents whether or not they have a SeMS. The incident response procedure is reactive, invoked when an incident occurs and the Framework focuses on adding a proactive dimension so that organisations can use the outcome of an incident to improve their security measures.

Incident response process

The incident response process within the SeMS should ensure continuous improvement. Continuous improvement may, amongst other means, be obtained by:

- conducting a review of the relevant parts of the incident response process after a full or partial exercise;
- debriefing and analysing the response operations after an incident; and
- developing new incident procedures or systems as part of the incident response process when new threats are identified by the SeMS.

Similar to preventive action building on corrective action (Chapter 5), the Framework builds on the incident response actions and outcomes to support a continuous improvement process. In the bullets it suggests three ways to do this:

1. incident response exercises are a rich source of information. Because they are conducted regularly in controlled conditions, they can provide considerable information about the robustness and performance of the incident response process with trends and comparative data from exercise to exercise.
2. Actual incidents may be less frequent and the data less complete than exercises, but the live data provides live operational information about security performance and any weaknesses.
3. When the SeMS identifies new threats, the incident response process should be tested against those new threats to determine what improvements are necessary or possible.

Understanding the SeMS Framework

Chapter 6 – Incident response

What the SeMS Framework says

Where appropriate, the Entity should co-ordinate its incident response processes with those of other interfacing organisations.

Why it says that

The primary benefit of co-ordinating the incident response process with partner organisations is to facilitate more effective management should an incident arise. However organisations can also take the opportunity to co-ordinate the three approaches discussed above, to gain from each other's continuous improvement benefits.

Initiating special security measures

Changing threat information or a security incident may require the urgent application of additional security measures or the suspension of operations.

The Entity should have a process for the urgent application of such additional security measures or suspension of operations.

The incident management process should include pre-planned procedures to invoke new measures or temporarily suspend operations that can no longer be secured.

Whilst the new procedures themselves cannot be planned in advance, the mechanism for invoking them should be, to make the invocation as quick and streamlined as possible.

Key points

1. The exercising of security incident response procedures can take many forms and can be of varying scale - the size of Entity largely determines how this is best achieved.
2. A log of outcomes and improvements subsequently made is good SeMS practice.

Incident response is invoked to handle incidents, occurrences, emergencies or events that are infrequent by their nature. It therefore needs to be exercised (and a record kept) periodically to test its continuing fitness. Exercises are also a valuable training tool and cultural influence.

Understanding the SeMS Framework

Chapter 7 – Management of change

What the SeMS Framework says

Why it says that

The SeMS should:

1. **Effectively plan, communicate, implement and measure the effect of changes to security policy and procedures**
2. **Monitor and measure the effects of change on security and facilitate action as appropriate**

In this chapter the Framework means any change, not just security changes. Big infrastructure change projects such as a redesign of a terminal will recognize the need for a security impact assessment, but smaller changes may not. It is as much a cultural and behavioural challenge as a procedural one, to get people to recognize when they are making a change and to consider any potential security impact in every change they make.

General principles

The Entity should manage the security risks related to a change. The management of change should be a documented process to identify external and internal change that may have an effect on security.

The organisation is likely to have processes to manage building, environment and technology changes. These could pose security risks, sometimes accidentally, and it is good practice to include a security impact assessment in the change planning stage.

However the organisation must be alert to changes which may not require significant physical work but which might have an impact on security – examples could include roster changes, introduction of new services, new partners, new destinations or changes in procedures by suppliers or partners.

The management of change

Change can introduce new risks and impact the appropriateness and/ or effectiveness of existing risk mitigation strategies. Changes may be external or internal to the Entity.

Having identified that a change is being planned, its impact on security and the SeMS itself, must be assessed. The project or person making the change may not be the best equipped to do this assessment: the security team should be consulted.

Understanding the SeMS Framework

Chapter 7 – Management of change

What the SeMS Framework says

The Entity should establish a formal process for the management of change which takes into account:

- the criticality of systems and activities;
- the stability of systems and operational environments; and
- past performance.

When business changes are planned the Entity should consider any impact on its SeMS through its security governance processes.

Why it says that

Any change where there is an identified impact on security should be managed carefully. This requires a change management process to have been created (and tested), so that the security impacts of the change can be managed through that process. The aspects to be considered include the bulleted list in the Framework.

All the above is true also of impacts on the SeMS. Using security governance processes ensures a fully-rounded business decision is made, favouring neither the security team nor the change proposer.

Key points

1. Change from any source can affect security. A robust SeMS will have clear change governance in place that will mitigate risk.
2. An internal culture that embraces security will minimise unintentional harmful impact on security.
3. Security needs to have a voice when change is being considered.

“Change” means any change, not just security changes. Big infrastructure change projects may recognize the need for a security impact assessment, but smaller changes may not. It is as much a cultural and behavioural challenge as a procedural one, to get people to recognize when they are making a change.

Understanding the SeMS Framework

Chapter 8 – Continuous improvement

What the SeMS Framework says

The SeMS should:

- Seek to improve security performance
- Evaluate all aspects of security provision
- Where appropriate, share security knowledge and skills

Why it says that

Security and the SeMS are not static. Security performance does not have a fixed target, because that will encourage an approach of doing the minimum necessary to achieve the threshold. This is counter to the SeMS philosophy and organisations should be doing whatever the risk assessment determines is needed. Since this is a management decision made up by weighing up all the factors including the cost of mitigations, it follows that any changes in efficiency or effectiveness of a process may change the cost/benefit balance in a previous risk decision. Changes in the organisation or externally tend to cause security decay – incremental degradation of effectiveness or efficiency – because they change the environment for which the security activities were originally designed.

Equally, changing external conditions such as threat levels, operational changes, economic situation etc may create new opportunities.

In response to these effects, the organisation should have a mechanism to seek improvement in the way security is done.

Continuous improvement

The Entity should seek to improve its security performance through proactive and/or reactive evaluation of the efficiency and effectiveness of:

- the Entity's security procedures;
- the Entity's facilities, equipment and documentation;

Evaluation, audits and continuous monitoring of how well security is working (for example monitoring the performance of risk mitigations) are a necessary part of the SeMS, necessary to security assurance. A secondary use of these activities and the information they produce is to identify where the SeMS itself can

Understanding the SeMS Framework

Chapter 8 – Continuous improvement

What the SeMS Framework says

- individual performance in the Entity, to verify the fulfilment of each individual's security responsibilities; and
- the Entity's system for control and mitigation of security risks. Where possible, data relating to the above points should be part of the evaluation.

Similarly the Entity should seek to improve its SeMS, as part of its security assurance, through actions such as:

- internal evaluations;
- independent audits (both internal and external); and
- continuous monitoring of security controls and mitigation actions.

Why it says that

be improved. For example the information on the performance of risk mitigations may also give insights into the effectiveness of the risk management process.

An equally, or perhaps more, valuable contribution to improvement may be available from the front-line staff. They know how security is actually done, not just what the book says, and they often know of shortcuts, obstacles and frustrations of their work.

Like quality circles in Quality Management, empowering the front line to make and test suggestions for security improvement can yield excellent results as well as being another cultural lever, engaging the staff in the future of security.

Sharing of information

Whilst aviation has mechanisms for sharing information on safety and on areas of weakness, this is not always the case in the area of security.

The Department for Transport and Civil Aviation Authority will encourage industry to bring forward ideas that lead to a greater sharing of information in ways that do not compromise the effectiveness of security or disclose sensitive information.

In particular, industry will be encouraged to collaborate on the development of new security management approaches, techniques and tools to assist in every Entity's continuous improvement.

Caution about the sensitivity of risk and breach information has prevented any significant advances in the sharing of information by organisations, but lessons can and should be learned from others' experiences. Shared information is a rich source of knowledge about an organisation's security and its SeMS, and the DfT and the CAA are expecting sharing to grow as SeMS are developed.

Information sharing is not limited just to performance data, but to every chapter of the SeMS. The pros and cons of one

Understanding the SeMS Framework

Chapter 8 – Continuous improvement

What the SeMS Framework says

Why it says that

organisation’s approach to third party contracts may be very helpful to another.

As SeMS become more comprehensively adopted, organisations need to be ready for and receptive to the CAA’s promotion of information sharing, anonymised where appropriate.

For example, an organization will find it helpful to know broadly how it ranks against its peers on any number of metrics, ways of working or quality of records.

Key points

1. A critical look at a SeMS by someone not directly involved can bring a fresh perspective and highlight gaps.
2. The sharing of information between SeMS entities will benefit everyone and help build security culture.

Front line people know how the job is actually done, not how management thinks it is done. Following the model of Quality Circles, empowering and supporting a volunteer “Continuous Improvement Circle” to develop ideas, can be a rich source of improvements. Including colleagues from other areas can be beneficial but is optional.

Information sharing is a rich source of ideas, but should not take precedence over the CI Circles.

Understanding the SeMS Framework

Chapter 9 – SeMS education and security culture

What the SeMS Framework says

The SeMS should:

1. Explain how the SeMS principles will be promulgated at all levels of the Entity
2. **Tailor** the relevance of the SeMS education provided
3. Evaluate the effectiveness of the SeMS on the Security Culture of the Entity

Why it says that

Culture and behaviour are mentioned many times in the Framework as a fundamental element of the SeMS. SeMS principles and other education must be given to ensure all staff are aligned on the SeMS, its importance and how it works.

The effectiveness of this education is of vital importance and should be monitored.

Aims and scope of training and education

SeMS education includes high-level awareness of SeMS, education in the concepts and principles of SeMS and detailed training in the processes and procedures of SeMS as required.

SeMS education should be relevant to:

- security culture;
- security assurance;
- security promotion;

The regulations deal with the security training requirements, but on top of those, training is needed about the SeMS itself. An effective SeMS requires all staff and third parties to understand and accept their responsibilities for security. Therefore SeMS education should cover a spectrum from concept and principles to the specifics and techniques for processes such as risk management.

The Framework picks out four topics for particular attention.

- Security culture is not something that can be manufactured; it has to evolve naturally and the role of education is to create the environment that promotes that evolution.
- Security assurance, the primary purpose of SeMS, represents a big cultural shift from compliance with regulations – which the training programme must explain and instill.

Understanding the SeMS Framework

Chapter 9 – SeMS education and security culture

What the SeMS Framework says

- security roles and responsibilities; and
- establishing acceptable levels of security.

The Entity should establish an education programme for all personnel, including all levels of management within the Entity (e.g. supervisors, managers, senior managers and the Accountable Manager), and ensure that the effectiveness of the programme is evaluated.

The amount and level of detail of SeMS Training should be proportionate and appropriate to the individual's responsibility and involvement in the SeMS.

SeMS education programme for the Entity's personnel

Why it says that

- Promoting the importance of security and the fact that security issues cross the whole organization is another part of that cultural shift.
- The practical impact of SeMS on roles and responsibilities also needs to be explained so it is fully understood.
- Unlike many aspects of compliance performance, which are binary (performance is either 100% or 0% compliant), SeMS is risk-based and 100% mitigation of risks is rarely achievable or desirable. In an effective SeMS, mitigation plans will be aimed at a level of security acceptable to management (having taken all things into consideration). The purpose of training is to explain this, not to set a particular target level of security, since the acceptable level will change as circumstances and capabilities change.

SeMS training is needed for all roles in the organisation, at the appropriate depth to suit the role. The effectiveness of the training must be evaluated in terms of the impact on attendees, and fed back to improve the training as necessary.

This section describes the training content for different roles in the organization. Training needs should be determined by analyzing the responsibilities of the individual being trained and this chapter should be read as a guide rather than a definitive list.

Understanding the SeMS Framework

Chapter 9 – SeMS education and security culture

What the SeMS Framework says

The programme should include the following, for each sub-set of personnel:

A. Operational personnel

- Security responsibilities, including adherence to all operating and security procedures, and recognising and reporting threats.
- Objectives should include familiarity with the Entity’s security policy and should ensure understanding of the Entity’s SeMS.
- How everyone can contribute to a positive Security Culture
- The contents should include, at a level of detail appropriate to the role:
 - (a) definition of threats;
 - (b) consequences and risks;

Why it says that

Operational personnel should be trained in their security responsibilities, including responsibilities within the regulations and within the SeMS. Whilst there may be specific training for certain aspects of the regulations, the SeMS training must at least refer to that training in order to demonstrate that the SeMS encompasses the regulations and is not an alternative to them.

The security policy, if constructed as discussed in Chapter 1, is likely to need some explanation – for example the rationale and the practical implications of the policy. To “ensure understanding of the Entity’s

SeMS” is a rather bigger objective, and is covered in the forth bullet point.

The education should show the desired culture but acknowledge that culture is not a subject that can be taught, it is a behavior to be encouraged by the right communication and leadership. Chapters 1 and 10 deal with this.

This list addresses the requirement to “ensure understanding of the Entity’s SeMS”:

- “What is a threat?” and how to search for threats.
- Definition and explanation of vulnerability and risk and how they fit with threats; and how threats are evaluated and mitigated.

Understanding the SeMS Framework

Chapter 9 – SeMS education and security culture

What the SeMS Framework says

Why it says that

- (c) the SeMS process, including roles and responsibilities; and
- (d) security reporting and the Entity's security reporting system(s).

- The whole Security Management System (Framework chapters 1 to 8), its processes and the roles in those processes, with the responsibilities of each role (to the appropriate level of detail).
- The requirements and process for security occurrence reporting.

Managers and supervisors

- Security responsibilities, including promoting the SeMS and Security Culture and engaging operational personnel in threat and incident reporting;
- In addition to the training objectives established for operational personnel, training objectives for managers and supervisors should include a detailed knowledge of the security process, threat identification and security risk management and mitigation, and change management.
- In addition to the programme specified for operational personnel, the education contents for supervisors and managers should also include security data analysis and the importance of quality assurance.

Training for managers and supervisors should cover the same ground as the training above for operational staff. Given that managers and supervisors have different and additional responsibilities (including those mentioned in this paragraph in the Framework), the content will not all be the same.

The objectives given in this paragraph in the Framework should be read as a general guide. A training needs analysis should be conducted to determine the actual requirement.

Data analysis is included because of the importance of performance monitoring in the SeMS (Framework chapter 5).

Senior managers

Understanding the SeMS Framework

Chapter 9 – SeMS education and security culture

What the SeMS Framework says

Why it says that

- Security responsibilities in relation to Aviation Security Requirements, as well as the Entity’s own security requirements, allocation of resources, ensuring effective internal security communication, active promotion of the SeMS Policy and development of a positive Security Culture.

As for managers and supervisors, so for senior managers in the organization. Given that they have different and additional responsibilities the content will not all be the same. In some areas, the level of detail will be less, but in others, including those mentioned in this paragraph in the Framework, the level of detail will be more.

Accountable Manager

- The SeMS Training should provide the Accountable Manager with a general awareness of the Entity’s SeMS, including SeMS roles and responsibilities, security policy and objectives, security risk management and security assurance and development of a positive Security Culture.

The Accountable Manager has different training needs. He/she needs a good understanding of corporate responsibility and how the SeMS helps directors deliver their fiduciary responsibilities, together with sufficient awareness of risk management and security assurance to fulfill the organisation’s accountability for security.

Key points

1. A SeMS can only fully deliver when an Entity has a positive and embedded Security Culture and awareness.
2. A SeMS education programme should reach everybody, and the message tailored to suit.
3. The sharing of information between SeMS Entities will benefit everyone and help build an industry-wide Security Culture.

The SeMS depends on, but also promotes an effective security culture – it shapes “the way we do things round here”.

The education must reach everybody and be aligned to their needs.

Culture is not only internal. Each industry and each sector has its own culture, and the influence of SeMS adopters will help that culture evolve. As in all innovations, the pioneers will have the greatest impact in shaping the future.

Understanding the SeMS Framework

Understanding the SeMS Framework

Chapter 10 – Communication

What the SeMS Framework says

The SeMS should describe:

- The means to effectively communicate security policy, requirements and priorities
- A process for measuring the effectiveness of those communications

Why it says that

Communication is management’s mouthpiece. The discussion of culture in “Understanding the SeMS Introduction” and cultural leadership in “Understanding Chapter 1 – Management Commitment” made it clear how important effective communication is in the development and maintenance of the right culture.

Security communication

The Entity should communicate the SeMS objectives and procedures to all relevant persons and organisations. The SeMS and its application should be evident in all aspects of the Entity’s operations.

Security communication should aim to:

- ensure that personnel are aware of the wider security responsibilities shared by all in the context of the entity’s Security Culture;
- ensure that all Relevant Personnel are fully aware of the SeMS;

Effective communication is a key tool in developing and maintaining the right culture. The aims listed here are intended to embed and reinforce that culture.

- Chapter 3 deals with defining responsibilities for each role, but those responsibilities must be communicated to the people expected to carry them out
- SeMS is based on the premise that all staff have a security responsibility, not just the security staff. The argument is that anybody could observe a security occurrence and should know what to do. This should be the starting point for all role definitions and training, but there may be some roles that do not have a bearing on security. To allow for that, the Framework refers to “all Relevant Personnel”. “Fully aware” means have sufficient awareness and expertise proportionate to the role.

Understanding the SeMS Framework

Chapter 10 – Communication

What the SeMS Framework says

- convey security-critical information;
- explain why particular actions are taken; and
- explain why security procedures are introduced or changed

Why it says that

- Staff need the information relevant to their responsibilities
- Explaining actions has three purposes: to provide information needed for the role, to educate and to promote the culture by enabling staff to see why an action was taken
- Explaining procedure changes has the same three purposes.

Communication tools

The Entity may use various tools to communicate security information, such as:

- the SeMS Manual;
- security processes and procedures;
- security newsletters, notices and bulletins; and
- websites or emails.

Communications should observe protective security markings and dissemination guidance as appropriate.

Regular meetings with personnel where information, actions and procedures are discussed may also be used to communicate security matters.

Organisations should plan communications carefully, using the channels and methods most suited to the audience and the message. The Framework lists the most common tools, but organisations will have others and should look for creative options to keep the message fresh.

Any information published should observe the appropriate confidentiality requirements.

In addition to the 'outbound' delivery methods, which are best suited to disseminating information, organisations may find two-way communications the most powerful means of getting belief and buy-in.

Key points

Understanding the SeMS Framework

Chapter 10 – Communication

What the SeMS Framework says

1. A good communications strategy will assist to embed SeMS and an active Security Culture.
2. Involving many areas of the business in contributing to communications builds inclusivity in security delivery.

Why it says that

Communications is as important as education in embedding SeMS and the right culture. Indeed much of the education will be delivered through communications channels. This is especially true of the mass education targeted at all personnel, not just the security staff. Most areas of the business will be involved in this, helping to make security an organisation-wide responsibility.