Introduction

What the SeMS Framework says…	Why it says that
Purpose	
A 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.	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 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.
A 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	There is no requirement in the regulations for an organization to have a SeMS. However there are quality control requirements in Articles

Introduction

What the SeMS Framework says…	Why it says that
help the Entity to meet the internal quality control provisions of articles 12, 13 and 14 of EC 300/2008[1].	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. 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.

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

Introduction

What the SeMS Framework says…	Why it says that
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.	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.
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 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. 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	The Framework describes the 10 components Chapter by Chapter, but

Introduction What the SeMS Framework says…	Why it says that
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 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.

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;	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

Chapter 1 – Management Commitment

What the SeMS Framework says…	Why it says that
• establish the Entity's security objectives and performance standards; and • determine and provide the necessary human and financial resources for the SeMS.	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: • be endorsed by the Accountable Manager; • identify security as a high organisational priority mutually supportive of commercial and operational priorities;	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.

Chapter 1 – Management Commitment

What the SeMS Framework says…	Why it says that
• reflect organisational commitments regarding security and the Entity's proactive and systematic management;	→ Explains how the positioning of security (previous bullet) is actually implemented – and is not just words.
• be communicated, with visible endorsement, throughout the Entity;	→ Reinforces visibility of management commitment – note that communication should be repeated creatively.
• include security reporting principles;	→ Explaining that security performance is to be measured and reported demonstrates that management is serious about SeMS.
• be periodically reviewed to ensure it remains relevant and appropriate to the Entity;	→ 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.
• include a commitment to: a) a continuous improvement programme;	→ 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.
b) ensure Aviation Security Requirements and all applicable standards are met, and consider best practices;	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) provide appropriate resources;	c) Providing the required resources is a pre-requisite of a successful SeMS. It is also a clear demonstration of management commitment.
d) enforce security as the responsibility of all personnel;	d) Making security the responsibility of the whole

Chapter 1 – Management Commitment

What the SeMS Framework says…	Why it says that
	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.
• include security reporting procedures (including access to the Anti-Terrorist hotline) and whistleblowing arrangements; and	→ 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.
• promote a positive security culture.	→ 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

Chapter 1 – Management Commitment

What the SeMS Framework says…	Why it says that
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.
The Accountable Manager should have a thorough knowledge and understanding of the key issues of risk management within the Entity.	Sponsoring SeMS requires a real understanding of risk management rather than detailed knowledge of the security regulations.
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	Tasks can be delegated; accountability cannot. The sponsor remains

Chapter 1 – Management Commitment	
What the SeMS Framework says…	**Why it says that**
Manager may delegate specified tasks. However, accountability and responsibility for those tasks remains with the Accountable Manager.	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.
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 SeMS. The Security Manager should: • 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 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 arrangements and while the SeMS may extend or bring extra intensity to them, the Framework aims not to duplicate anything.
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	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.

Chapter 1 – Management Commitment	
What the SeMS Framework says…	**Why it says that**
• 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.	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.

Chapter 2 – Threat and risk management	
What the SeMS Framework says…	**Why it says that**
Local threat identification process 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/attachme	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.

Chapter 2 – Threat and risk management What the SeMS Framework says…	Why it says that
nt_data/ file/11516/guide.pdf	
Assessing vulnerabilities	
The threat and risk assessment process should capture a clear and comprehensive picture of where vulnerabilities may 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	
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.	In this section the Framework outlines the typical stages of a risk assessment process.
Security risk assessment is the analysis of the security risks of the consequences of the threats that have been determined.	The highlights of risk management, including risk assessment, are described in the SeMSnet document ‘Risk Management Primer’.
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. Security risk decision making and acceptance should be specified by the Entity through a risk tolerability matrix.	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	

Chapter 2 – Threat and risk management What the SeMS Framework says…	Why it says that
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.

Chapter 3 – Accountability and responsibility What the SeMS Framework says…	Why it says that
Defined accountability and responsibilities The Entity should define accountability and responsibilities for security throughout the Entity, including security governance responsibilities at all levels.	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

Chapter 3 – Accountability and responsibility

What the SeMS Framework says…	Why it says that
	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 the SeMS is effective. 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; • 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.	In order for the Accountable Manager to discharge his/her responsibilities, there must be a governance mechanism that gives the Accountable Manager and management above him/her the ability to drill down and control the SeMS. This section outlines the requirements for the governance mechanism. These are summarised in the four bullets: • 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 • 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.
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 described[4].	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. Note that the URL referenced in the footnote is out of date. The latest

Chapter 3 – Accountability and responsibility

What the SeMS Framework says…	Why it says that
Other Entities are encouraged to adopt a similar approach where appropriate.	location is https://www.gov.uk/government/publications/airport-security-planning-quick-guide

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 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

Chapter 4 – Resources

What the SeMS Framework says…	Why it says that
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	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

Chapter 4 – Resources

What the SeMS Framework says…	Why it says that
• implement and maintain the security processes that deliver the SeMS, the Aviation Security Requirements and any other risk mitigation identified.	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 contributing to a security process should be competent and have appropriate education, training, skills and experience. 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.	Personnel – staff, contractors and third party suppliers' staff – are one of the key resources that should be determined by 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	

Chapter 4 – Resources What the SeMS Framework says…	Why it says that
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.
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.	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 could affect aviation security, it should, where possible, specify any security-related requirements, including the provision of information, 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 3rd party 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.

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says...	Why it says that
Performance monitoring and measurement process	
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. This process should include the setting of security performance indicators and security performance targets and the measurement of the security performance against them. Security key performance indicators should be identified to inform all levels of relevant management in the Entity. The performance monitoring and measurement process should include: • addressing the performance in relation to the Aviation Security Requirements; • 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; • examination of particular elements or procedures of a specific operation; and	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 • 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 • Performance reports, trends or audits may identify areas needing examination

Chapter 5 – Performance monitoring, assessment and reporting	
What the SeMS Framework says...	**Why it says that**
• internal security investigations of security incidents.	• 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.	The next two sections deal with corrective actions (putting right failures) and preventive actions (stopping failures occurring).
Any corrective actions should be appropriate to deal with the effects of the poor performance identified by the Entity.	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.
A documented procedure should be established to define requirements for: • reviewing poor performance; • determining the causes of poor performance; • evaluating the need for action to ensure that poor performance does not recur;	The bullets describe the components of the corrective action procedure, namely: • investigate what happened • identify what caused it • determine whether preventive action is also required (see next section for preventive action)

Chapter 5 – Performance monitoring, assessment and reporting	
What the SeMS Framework says...	**Why it says that**
• determining, implementing and recording the appropriate action; and • reviewing corrective action taken.	• 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.	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.
A documented procedure should be established to:	The bullets describe the components of the preventive action procedure, namely:
• determine potential poor performance and its causes;	• 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
• evaluate the need for action to prevent occurrence of poor performance; • determine, implement and record the appropriate action; and review preventive action taken.	• 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 action); review the effectiveness of the preventive actions after they have had time to take effect

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says...	Why it says that
Management of security data and information	
The objective for management of security 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 decribes the security 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 and 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, where appropriate, so that others may learn from them.	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 • having procedures or tools to share across the organisation the knowledge gathered by the reporting system and the lessons learnt
The Entity should identify which events are to be reported.	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

Chapter 5 – Performance monitoring, assessment and reporting

What the SeMS Framework says...	Why it says that
	certain incidents and occurrences mandatory.
The security reporting system should have the capability to confirm receipt to the reporter, where appropriate.	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.
The reporting process should be simple and clearly defined including details as to what, how, where and when to report.	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.
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.	The incident and occurrence data must be capable of being accessed by authorised analysts (subject to appropriate access controls) to enable meaningful analysis.
Access to the submitted reports should be restricted to protect the identity of the source, where appropriate.	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.
The security reporting system should include a feedback system to the reporting person on the outcome of the occurrence analysis.	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 security reporting system should also include a voluntary confidential reporting process for reporting security matters.	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

© 3DAssurance Ltd 2017

Chapter 5 – Performance monitoring, assessment and reporting	
What the SeMS Framework says...	**Why it says that**
	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. 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	
The quality of security-related data and information should be assured by a quality management system that controls the origination, production, storage, handling, processing, transfer and distribution of that data and information.	The previous section dealt with storage and protection of security data. This section adds the requirement to assure the 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

Chapter 5 – Performance monitoring, assessment and reporting	
What the SeMS Framework says...	**Why it says that**
	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.

Chapter 6 – Incident response	
What the SeMS Framework says…	**Why it says that**
Incident response	
The SeMS should include response processes for dealing with security incidents. The processes should be exercised or reviewed as appropriate on a regular basis.	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:	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:
• conducting a review of the relevant parts of the incident response	1. incident response exercises are a rich source of information.

Chapter 6 – Incident response	
What the SeMS Framework says…	**Why it says that**
process after a full or partial exercise; • debriefing and analysing the response actions 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. Where appropriate, the Entity should co-ordinate its incident response processes with those of other interfacing organisations.	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. 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.

Chapter 7 – Management of change

What the SeMS Framework says…	Why it says that
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.	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 consider any potential security impact in anything they do.
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.
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.	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.
When changes are planned the Entity should consider any impact on its SeMS.	All the above is true also of impacts on the SeMS.

Chapter 8 – Continuous improvement

What the SeMS Framework says…	Why it says that
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; • 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.	This chapter deals with continuous improvements to both security performance and SeMS. 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. The bullet points list areas that should be assessed in this way.
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); • strict document controls; and • continuous monitoring of security controls and mitigation actions.	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 be improved. For example the information on the performance of risk mitigations may also give insights into the effectiveness of the risk management process.
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.	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'

Chapter 8 – Continuous improvement

What the SeMS Framework says…	Why it says that
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 sensitive information.	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.
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**.**	Information sharing is not limited just to performance data, but to every chapter of the SeMS. The pros and cons of one 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.

Chapter 9 – SeMS Training and education

What the SeMS Framework says…	Why it says that
### Aims and scope of training and education	
SeMS Training includes high-level awareness of SeMS, education in the concepts and principles of SeMS and detailed training in the processes and procedures of SeMS.	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

Chapter 9 – SeMS Training and education

What the SeMS Framework says…	Why it says that
	cover a spectrum from concept and principles to the specifics and techniques for processes such as risk management.
SeMS Training should be relevant to: • security assurance; • security promotion; • security roles and responsibilities; and • establishing acceptable levels of security.	The Framework picks out four topics for particular attention. → Security assurance, the primary purpose of SeMS, represents a big cultural shift from compliance with regulations – which the training programme must explain and instill. → 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 if 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.
The Entity should establish a training 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 SeMS Training is evaluated.	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.
The amount and level of detail of SeMS Training should be	

Chapter 9 – SeMS Training and education

What the SeMS Framework says…	Why it says that
proportionate and appropriate to the individual's responsibility and involvement in the SeMS.	
SeMS Training for the Entity's personnel **Operational personnel**	
The SeMS Training should address security responsibilities, including adherence to all operating and security procedures, and recognising and reporting threats.	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. 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 training objectives should include the Entity's security policy and should ensure understanding of the Entity's SeMS.	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, requiring at least the following:
The contents of the SeMS training should, at a level of detail appropriate to the role, include: • definition of threats; • consequences and risks; • the SeMS process, including roles and responsibilities; and	→ "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. → The whole Security Management System (Framework chapters

Chapter 9 – SeMS Training and education

What the SeMS Framework says…	Why it says that
• security reporting and the Entity's security reporting system(s).	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	
SeMS Training should address security responsibilities, including promoting the SeMS and engaging operational personnel in threat and incident reporting.	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.
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.	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.
In addition to the contents specified for operational personnel, the training contents for supervisors and managers should also include security data analysis.	Data analysis is included because of the importance of performance monitoring in the SeMS (Framework chapter 5).
Senior managers	
SeMS Training should include 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, and active promotion of the SeMS.	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.

© 3DAssurance Ltd 2017

Chapter 9 – SeMS Training and education

What the SeMS Framework says…	Why it says that
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.	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.

Chapter 10 – Communication

What the SeMS Framework says…	Why it says that
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; • ensure that all Relevant Personnel are fully aware of the SeMS;	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. 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

© 3DAssurance Ltd 2017

Chapter 10 – Communication What the SeMS Framework says…	Why it says that
	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.
• convey security-critical information; • explain why particular actions are taken; and • explain why security procedures are introduced or changed.	→ 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.
There should be a process for measuring or assessing the effectiveness of the security communications.	Given the dependence on communications to inform and to motivate, it is essential to confirm it is effective, and where it is not, to improve it.
Communication tools	
The Entity may use the following tools to communicate security information: • the SeMS Manual; • security processes and procedures; • security newsletters, notices and bulletins; and • websites or emails.	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.
Communications should observe protective security markings and dissemination guidance.	Any information published should observe the appropriate confidentiality requirements.

Chapter 10 – Communication	
What the SeMS Framework says…	**Why it says that**
Regular meetings with personnel where information, actions and procedures are discussed may also be used to communicate security matters.	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.