



# PARAS

PROGRAM FOR APPLIED  
RESEARCH IN AIRPORT SECURITY



PARAS 0009

March 2018

## Guidance for Security Management Systems (SeMS)

**National Safe Skies Alliance, Inc.**

Sponsored by the Federal Aviation Administration

**Renè Rieder, Jr.**  
**Stacey Peel**  
**Liz Swinstead**  
Arup  
New York, NY

© 2018 National Safe Skies Alliance, Inc. All rights reserved.

#### **COPYRIGHT INFORMATION**

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

National Safe Skies Alliance, Inc. (Safe Skies) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply Safe Skies or Federal Aviation Administration (FAA) endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from Safe Skies.

#### **NOTICE**

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

## **NATIONAL SAFE SKIES ALLIANCE, INC.**

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about airport security technologies and procedures.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying perimeter and access control security technologies and procedures.

Through the Program for Appplied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

## **PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY**

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at [www.sskies.org/paras](http://www.sskies.org/paras).

---

### **PARAS PROGRAM OFFICER**

**Jessica Grizzle** *Safe Skies Special Programs Manager*

---

### **PARAS 0009 PROJECT PANEL**

**Thomas Anthony** *University of Southern California*

**Frank Capello** *Broward County Aviation Department*

**Dawn Lucini** *Telos Identity Management Solutions, LLC*

**Timothy O’Krongley** *Garver, LLC*

**Charlotte Peed** *CP2*

**Jeremy Worrall** *State of Alaska Department of Transportation*

# Contents

---



## You are here

<b>1</b>	<b>Getting to know SeMS</b>	
1.1	Project background	3
1.2	Introduction	4
1.3	Using this Guidance	7
1.4	SeMS at a glance	12
<b>2</b>	<b>Are you SeMS ready?</b>	
2.1	Assessing your SeMS readiness	40
2.2	What is your readiness starting point	42
2.3	Proceeding with an SeMS	43
2.4	Now you know your SeMS readiness, what's next?	48
<b>3</b>	<b>How to establish your SeMS</b>	
3.1	Introduction to how to establish your SeMS	50
3.2	What is the SMAT?	51
3.3	How do I use the SMAT?	56
3.4	Interpreting your SMAT results	69
<b>4</b>	<b>APPENDICES</b>	<b>79</b>



# Project background



National Safe Skies Alliance commissioned Arup to develop "...a single guidance document that addresses the purpose, applicability, and implementation of an SeMS that will assist airport operators in enhancing their security posture." This SeMS User Guidance document (hereafter Guidance) is the product of that commission.

The Guidance has been written with a human-centered design approach; future users were consulted early in its development, influencing both content and format. Consultation involved a series of interviews, a validation workshop, and Project Panel reviews. The interviews and validation workshop were held with personnel who work in airports, including employees of organizations who work at airports but who are not employed directly by the airport; employees who are employed directly by the airport; non-security personnel; and employees with designated security roles.

The Guidance has been developed specifically for the US airport market and is intended to be scalable, i.e., usable by large, small, city, regional, and complex airport operations.

The Guidance is not intended to be a security handbook and will not provide procedures for security implementation (e.g., incident response or training material). It is intended to increase your airport's SeMS knowledge and guide you on implementing and maintaining an SeMS in a way that is conducive to real change and improvement to your security outcomes.



This Guidance has been developed for those individuals, teams, or task forces who are responsible for establishing and maintaining an SeMS at their airport. Its purpose is to:

- 1 Help you to understand SeMS
- 2 Inform you of the benefits of SeMS
- 3 Help you determine whether your airport is ready to establish an SeMS and determine next steps depending on your SeMS readiness level
- 4 Guide you on establishing an SeMS
- 5 Inform you of the governance required to establish and maintain the SeMS
- 6 Guide you on how to undertake quality assurance of the SeMS

## What is an SeMS?

An SeMS is a mechanism or management technique to establish and maintain a security culture, and to integrate security into the airport’s business. The security culture is utilized to manage security risks, while the inculcation of security into the business provides for more effective, efficient, and sustainable security. The culture aspect is consistent with the Safety Management System (SMS) experience, which has proven that a positive safety culture results in improved safety through the reduction of safety hazards.

The establishment and maintenance of an airport-wide security culture and the integration of security into the airport’s business are achieved by establishing and maturing seven Elements that, when integrated with each other and the broader airport business, form a system—an SeMS. The individual Elements are deemed critical components to security that, when working as a system, provide for collectively improved security outcomes.

Figure 1-1 illustrates an SeMS. It shows the individual Elements, their relationship to each other, the governance and quality assurance that underpins the system’s functionality, and their collective contribution to a positive security culture. ‘Becoming familiar with SeMS’ provides more detail about the system itself, and further detail about the individual Elements is in Appendix A.



# Introduction

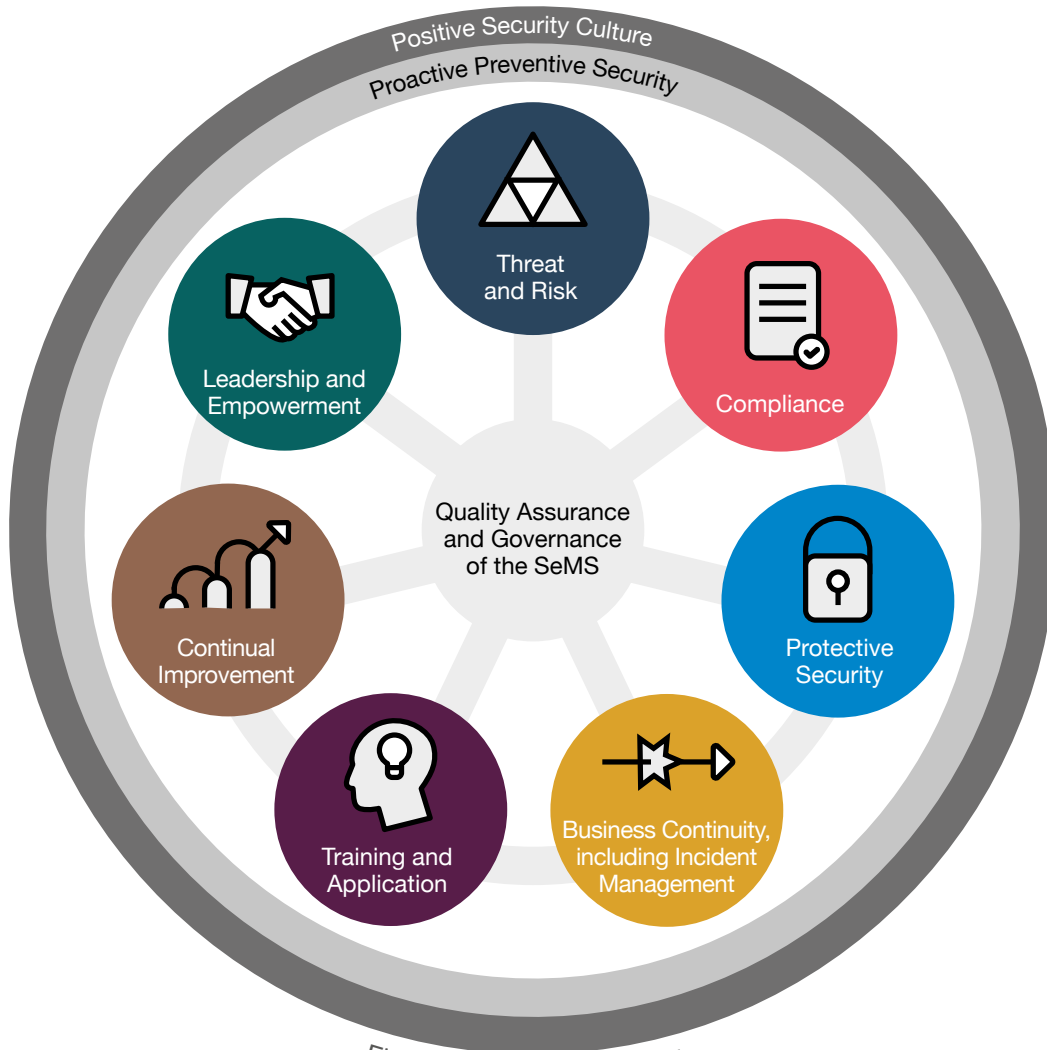


Figure 1-1. SeMS Elements



# Introduction

---

The following examples show SeMS in action.

## Example

The Airport Operations Center (AOC) analysis of monthly reports from the door alarm system identifies a trend associated with failed and successful attempts to access a particular Security Restricted Area (SRA). This includes attempts by personnel who are currently on performance management programs. They have been advised that if they are caught entering unauthorized areas again, they can be dismissed. Through consultation with the Airport Security team, it is learned that the area has recently been established as an SRA; however, this has not been communicated to airport staff. A targeted communication is issued, and the unauthorized access attempts cease. No warnings are issued to personnel. This example demonstrates the Leadership and Empowerment (not defaulting to penalizing staff), Continual Improvement (root cause analysis of the breaches), Protective Security (SRA), and Compliance (regular system reporting) Elements of an SeMS working together. It also demonstrates security being integrated within the different areas of business, namely AOC, Security, Human Resources, and Communications.

## What an SeMS is not

Designers of SeMS have drawn on the lessons learned from the SMS experience, in particular, the value of culture in identifying and managing safety hazards and risks. However, unlike an SMS, an SeMS also focuses on integrating the management of security into the other facets of airport business. This characteristic of SeMS is more like a Quality Management System (QMS). In fact, because of the systemic nature of their operations, SeMS, SMS, and QMS are complementary. A comparison between SeMS and SMS can be found in Appendix B.

An SeMS is not a library of security-related documentation. While an SeMS drives a systems approach to security, and good documentation management is one of its many features, creating a library of security-related documentation alone will not result in a positive security culture, nor will it integrate security into the broader airport business. This Guidance provides cross references to documents that you might typically feature in your SeMS (e.g., Airport Security Program).

An SeMS is not an electronic system that provides a single interface of all electronic security systems. While such an integrated security system might form part of an SeMS and help facilitate the integration of security into the business (e.g., using security CCTVs to assist with improved Special Assistance Accessibility), it is not an SeMS.

An SeMS is not an additional requirement process or check to be overlaid on the business. An SeMS is fundamentally about culture and business management, and therefore, by its very nature, is integrated into the functions of the airport and the attitudes and mindset of the airport community.

The extent to which you use this Guidance will depend on the SeMS-readiness of your airport.



The 'Are you SeMS ready?' section will guide you on determining that. Based on the outcome of that simple self-assessment you will move on to using a little, or a lot, of The Guidance.

The most effective approach is to:

<p><b>1</b> Familiarize yourself with SeMS</p>	<p>Refer to Section 1 'Getting to know SeMS'</p>
<p><b>2</b> Determine your airport's SeMS readiness</p>	<p>Refer to Section 2, 'Are you SeMS ready?'</p>
<p><b>3</b> Follow the guidance/ next steps provided in Section 3 in accordance with the outcome of that assessment</p>	<p>Subject to the outcome of your SeMS readiness assessment, you will be:</p> <ul style="list-style-type: none"> <li>• Using the material in this Guidance to only raise awareness and knowledge of SeMS.</li> <li>• Building a case for action and creating structure and priorities for action by conducting a maturity self-assessment using the SeMS Maturity Assessment Tool (SMAT) provided with this Guidance.</li> <li>• Starting to design and implement an SeMS for your airport by understanding your current SeMS maturity using the SMAT, using this Guidance material to prioritize actions, and developing an SeMS Implementation Plan.</li> <li>• Conducting quality assurance of your existing SeMS and responding accordingly. You might also consider sharing your SeMS experience with other airports.</li> </ul>



# Using this Guidance

---

## Why would you want to implement an SeMS?

Current security approaches may not provide the best security or monetary return on investment.

Historically, aviation security measures have been adopted in response to security events, i.e., after security incidents have already occurred. This reactive approach has resulted in the application of security measures that can incur significant capital and operating expenditures. These expenditures may have been less had a more proactive approach been taken. A reactive approach can also have an adverse impact on other business objectives, such as passenger experience and architectural design.

If driven by regulatory requirements, security measures are often one-size-fits-all. As a result, these measures might not always reduce or eliminate the security risk being targeted, or might ignore more significant risks and vulnerabilities that exist due to an individual airport's unique infrastructure and operations.

There has also been a historic reliance on technology to manage security risks. This tendency can result in a blind spot, which is the lack of attention to human resources. Humans are able to identify and address risks in a more agile, intelligent, and, at times, intuitive manner when compared with relying purely on technology. Building such human capability may be relatively cheap in the long run, and result in a greater ability for the airport to stay ahead of ever-evolving security risks and threats.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Using this Guidance

### How SeMS improves security and business

Using humans in the reactive security solution is not uncommon, for example, the employment of security guards. However, in the case of security guards, their capability to identify and address risks is limited to the geography of their roles. Their attention and intuition may also be inhibited by their duties and usual workload. Establishing a security culture that touches each and every person who works at or is in close association with an airport provides an enhancement—a security-fabric, of which every human in the airport system is a thread.

This security fabric exists across the entire airport’s footprint, and at times beyond that footprint, and it exploits the human intuition associated with risk management. Additionally, the identification and addressing of risks can occur significantly faster than security measures that require a manufacturing and installation lead-time.

**“Before the active shooter incident, people in our airport intellectually knew security was important. Now they believe it in their hearts.”**

2017, Interviewee, employed at large US airport

#### Example

Patrolling security guards cover a large area during their shift. They typically pass through a particular area a number of times for a short period each shift. For example, they may pass by the café four times in that shift and be in that area for around 30 seconds each time. The security guards therefore see that area for 120 seconds, or 2 minutes, over an 8-hour shift.

In contrast, the 4 staff members who work in the café spend their entire shift in the same area and would therefore each see that area for 7.5 hours in an 8-hour shift. It makes sense that those four staff that work at the café are very familiar with the area and therefore will identify activity that is unusual for that space.

If we take this example further, and consider it in the context of a small airport, we can quickly see how an environment in which many people know each other, possibly hold multiple roles, and know the habits and routines of the airport, will be in a position to be a powerful ‘eyes and ears’ network beyond those tasked with formal security roles.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Using this Guidance

In addition to improving security, an SeMS can provide other benefits by breaking down silos across the business, sharing resources, and applying a systems approach to decision making. Examples include:

- Reduced capital expenditure through a risk-based, total-design approach to all infrastructure projects
- Reduced operational expenditure through a risk-based, total-design, whole-life approach to reducing security risks
- Reduced insurance costs
- Increased sense of community as different stakeholders in the airport collaborate to enhance security for everyone
- Improved general workforce engagement through the effective implementation of Leadership and Empowerment Elements of SeMS
- Improved hazard identification; when people are attuned to identifying risks and feel empowered to do something about those risks, they are likely to identify other types, such as safety risks
- Independent accreditation and recognition, such as SABRE accreditation
- Improved business resilience as the system provides established networks, communications, and mechanisms, (e.g., one airport reported that coordination of response activities and dissemination of information associated with Hurricane Irma was more efficient than for past incidents because a network of communication was already established through their SeMS)
- Reduced security cost through existing business mechanisms, e.g., using the airport's talent program to establish a career path for security personnel, or using the airport's staff-only cell phone app to disseminate time-critical information like change in threat level

A detailed Case Study can be found at Appendix C.

**Culture can be dysfunctional if the shared values of the staff are not aligned with the values and objectives of the organization. If the workplace culture does not encourage, support and value security, no security management system can succeed in improving. As each new security procedure or initiative is introduced, the reigning culture will determine new ways to avoid complying and continue doing things the way we do things round here.**

Queensland Mining Industry Health and Security Conference Proceedings – 1999



SeMS components are:

- 1 Seven Elements (that work together)
- 2 Governance (that informs the SeMS establishment and maintenance)
- 3 Quality Assurance (that informs the SeMS's ongoing effectiveness)

This section provides some detail on those components.

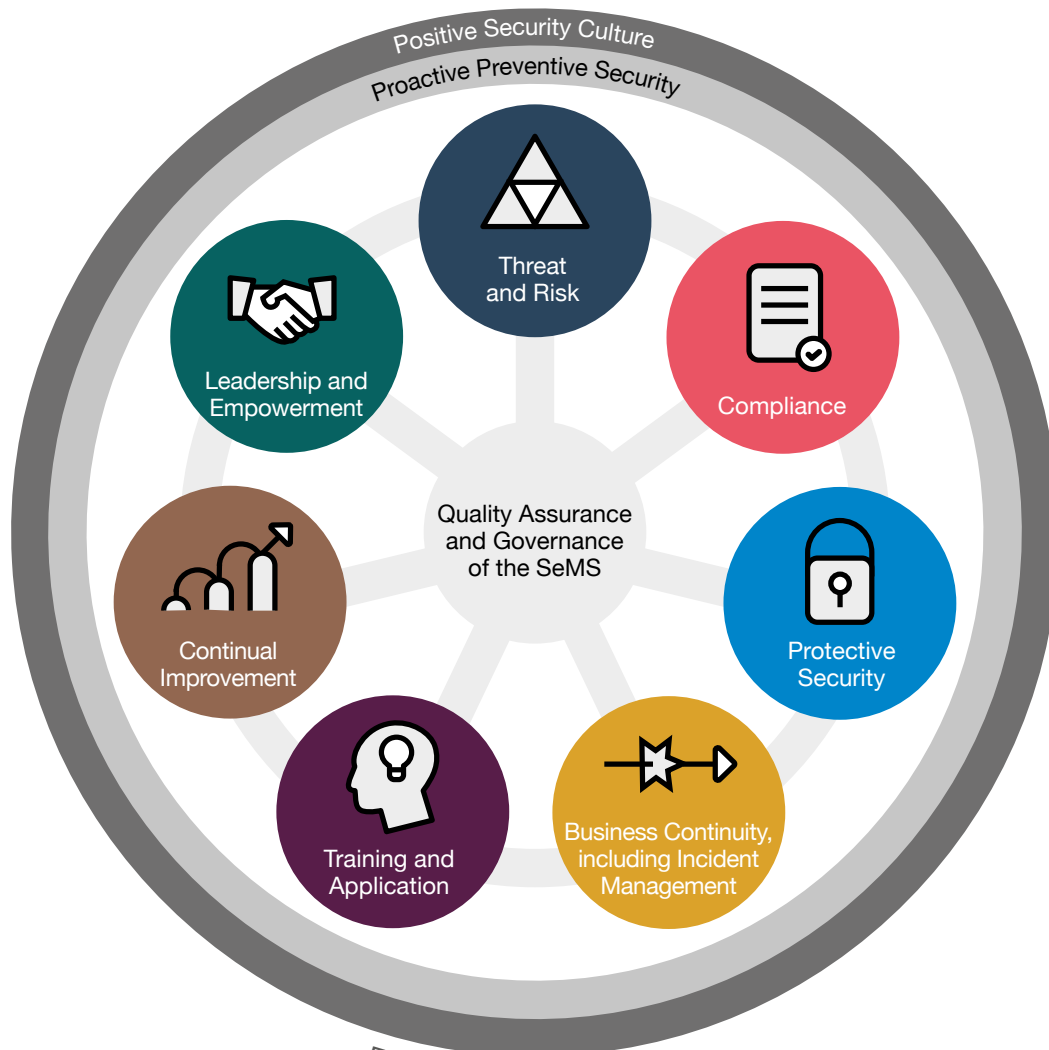


Figure 1-1. SeMS Elements





## Governance of SeMS

While the spirit and intent of an SeMS is that it is integrated into the airport's business, its establishment will require a change-management approach, thus demanding governance-related resources.

The resources expected for SeMS establishment and maintenance is likely to be limited to personnel (versus finance). The nature of an SeMS suggests that staff members involved in its establishment are already an integral part of the business. The time required of those staff members for SeMS establishment and maintenance will depend upon your airport size, the staff members' existing roles and responsibilities, their current capabilities, and current airport SeMS maturity and maturity aspirations.

**“Key central influencers need to be on board early on – e.g., specific supervisors, people whose voices carry weight (informally).”**

2017, Interviewee, employee from small US airport

It is recommended that an SeMS Champion and SeMS Facilitator be identified.

The SeMS Champion is someone at the executive level who champions the changes required to establish the SeMS and leads by example. While the SeMS Facilitator is likely to be someone from the security team, it may be appropriate that the SeMS Champion is from another part of the business, e.g., Chief Operating Officer. The priority is that the SeMS Champion is someone who is willing and capable to make the critical changes needed in order to have security integrated into the business. Because this may mean making changes to parts of the business other than security, an SeMS Champion from another part of the business may be better positioned to do so than senior security personnel.

In considering who should take on the SeMS Champion role, you should also consider the knowledge, skills, attributes, experience, and competencies needed:

- Is the person a persuasive speaker who is able and willing to clearly articulate the case for an SeMS?
- Does the person build a good network and good relationships in the airport and beyond, understand the challenges and opportunities for change within the airport, and connect to a wide range of airport stakeholders at a senior level?
- Does the person hold a position of formal authority, so that when their name appears on an email, or when they ask for a meeting, people consider their message to be important and worth making time for?
- Does the person grasp the financial and commercial implications of decisions made to implement an SeMS, and is that person familiar with concepts such as threat, risk, business impacts, and links between an SeMS and overall airport/business strategy?



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# SeMS at a glance



The SeMS Facilitator is someone who is responsible for administering the SeMS, and is most likely to come from the security team. In smaller airports, or airports where roles are less specialized, this person may not come from a security department, but may wear a security hat as part of other roles that they hold. The Facilitator's work will involve:

- Educating those involved in the SeMS establishment
- Working with the SeMS Champion to facilitate strong support for the SeMS in the form of demonstrable culture change and commitment of resources (where necessary) to mature particular Elements
- Leading the SeMS Maturity Self-Assessment (described later in this document)
- Empowering leaders in the business to lead on necessary culture-change management and tool-establishment/adoption of initiatives
- Leading the quality assurance of the SeMS
- Providing guidance on the promotion of the SeMS
- Acting as the project director or manager (subject to scale) if an SeMS improvement or transformation project model is adopted

In considering who should take on the SeMS Facilitator role, you should also consider the following traits:

- Have a willingness to pursue security outcomes through disciplines other than security-specific solutions?
- Show persistence and resilience, and able to recover from setbacks?
- Able to turn broad concepts into defined activities and plans of work?
- Readiness to track activities, follow-up actions and collect data?
- Commitment to working through relationships and bringing people along in the most appropriate manner, depending on SeMS maturity?
- Influence without large amounts of formal, positional, authority? This may be through relationship building, articulating clear benefits cases, assertively highlighting key issues.
- Develop and deliver well written and verbalized communications materials and presentations?
- Use tools such as Microsoft Excel and Word to track implementation progress and develop reports?
- Have deep knowledge of the airport community and the way the airport functions?



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



## Quality Assurance of SeMS

Quality Assurance is the system that determines the ongoing effectiveness of the SeMS. It comprises a quality assurance process and metrics. The quality assurance process involves regularly assessing the SeMS performance against criteria/metrics agreed to by the organization.

Refer to Appendix D for guidance on the quality assurance process and the value of metrics for SeMS sustainability.

## Individual Elements of an SeMS

An SeMS comprises seven elements that work together:

- 1 Threat and Risk
- 2 Compliance
- 3 Protective Security
- 4 Business Continuity, including incident management
- 5 Training and Application
- 6 Continual Improvement
- 7 Leadership and Empowerment

The effectiveness of each Element's contribution to an SeMS is dependent upon the maturity of the tools used to operate the Element and the mindset associated with the Element.

Tools can be defined as the mechanisms that facilitate the Elements' intent. An example of a Compliance tool is an audit checklist.

Mindset can be defined as the organization's belief in the value of the Element's intent (i.e., the widespread and common understanding of the Element's intent and active use of tools to facilitate its manifestation). An example of a (positive) Compliance mindset is a belief that the compliance activity, e.g., audit, is only complete when the action to correct deficiencies has been confirmed (versus complete when the audit findings are recorded). This stems from a deeply held belief that Compliance activities in general are in service of making sure that actions are carried out to genuinely improve security outcomes (contrast this against the belief that Compliance is there to look good, check the box, or cover our backs).

Recognizing that each Element consists of tool(s) and mindset is critical to this Guide's use. This is because improving an Element's contribution to an SeMS will be dependent upon the need to address the tool or the mindset associated with that Element. It is possible to have robust tools but not an adequate mindset (and vice versa), resulting in the entire Element being less than effective.



# SeMS at a glance



Continuing with the Compliance example:

## Example

The Security Team has developed a quality control system that comprises quality control checklists, audit training for inspectors, a quality control findings database, and communication templates, e.g., notification of audit and the audit finding report.

Given these tools, one could expect that Compliance is effective at their airport.

However, the annual internal audit is the only quality control activity undertaken, and is undertaken only when a (Transportation Security Administration) TSA audit is scheduled; senior airport management treats the findings as low priority and seeks to suppress any adverse finding. Last year's TSA findings are not considered in any corrective action.

The airport has mature Compliance tools but lacks an effective and positive Compliance mindset. It is not difficult to understand why the airport does not have good compliance.

It is clear that to improve Compliance, more effort should be given to improving the mindset compared to the effort given to improving tools.

The following describes each Element, including some indicator of 'what good looks like'. What good looks like reflects the value of both mindset and tools.



1  
Getting to know  
SeMS

2  
Are you  
SeMS ready?

3  
How to establish  
your SeMS

4  
Appendices



# SeMS at a glance

## Threat and Risk

---

Threats are individuals with the intent and capability to undertake an act of unlawful interference. Unlike other types of risks (e.g., safety), the threat in the security context has the capability to and will actively:

- Avoid risk mitigation measures, e.g., bypass security measures such as screening
- Seek out and exploit vulnerabilities, e.g., attack unprotected areas such as landside

Risk is the manifestation of an act of unlawful interference measured by the likelihood of the event occurring (taking into account vulnerabilities) and the consequences if the event occurs.

### Example

The threat is known to have the capability and willingness to use automatic weapons in an attack. Automatic weapons are relatively easy to procure given the law in this airport's state. Therefore, relative to other states with stricter regulations, the occurrence factor will increase for an airport in this state, raising its risk.

An SeMS is ultimately about reducing an airport's exposure to security risks by identifying the security risks and subsequently managing them.

### What good looks like

While not an exhaustive list, the following describes a few examples of what 'good' might look like:

- All of the airport community is alert to identifying and reporting vulnerabilities.
- There is a formal risk management process and framework in place, and both are being used.
- The differences between risk management and compliance are widely understood.
- Threat and risk briefings are a standing item on the Executive and Board meeting agenda.
- Security is an integral part of the airport's enterprise risk management framework.

For more information about Threat and Risk, refer to Appendix A.



# SeMS at a glance

## Threat and Risk



The following is a non-exhaustive list of indicators that suggest improvement might be needed in your airport's Threat and Risk tools and/or mindset:

- There is no reporting system in place that allows the airport community to (confidentially) report suspicious activity.
- Priority is given to addressing compliance issues rather than addressing security vulnerabilities.
- No regular risk assessment, including vulnerability identification, is conducted at the airport.
- There is little to no engagement with the government agencies that provide threat information.
- Security risk does not appear on any Airport Executive meeting agendas.
- Security measures are only implemented and reviewed when an instruction from authorities is received.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# SeMS at a glance

## Compliance



Compliance is the act of conforming to national aviation-security-related regulations. The security processes and measures imposed by regulations are the minimum that the airport must apply. The effectiveness of those measures should be taken into account in the risk assessment. Application of those security measures will not address all risks that are relevant to the airport, hence the Threat and Risk Element. It is, however, a necessary element of a security system given the federal requirements.

Airports will be subject to compliance checks by the TSA. Airports may also be subject to compliance checks by other third parties who have an interest in the impact of the airport's security on their own security/operations (e.g., airlines and governments of other states that are the destinations of departing flights). Additionally, airports should have their own internal quality control arrangements in place to self-assess their compliance. Compliance activities include:

- 1 Audit
- 2 Inspection
- 3 Test
- 4 Exercise
- 5 Survey

### What good looks like

- An internal quality control system is in place to conduct a self-assessment of compliance.
- The frequency and types of compliance activities are informed by risk (refer to Threat and Risk).
- The compliance process is focused on improving security, not just checking boxes.
- Compliance activities are welcomed and considered an opportunity to improve.
- Compliance takes into account effectiveness of measures (not only their existence).
- Compliance includes ensuring the corrective action arising from adverse compliance findings is undertaken, (i.e., it is not assumed that once the site-visit audit has been done, the compliance activity is finished).
- A quality control system is in place and comprises a schedule of quality control activities (including follow-up on corrective action), guidance for inspectors, inspector authority, competent inspectors, a quality control finding database, enforcement policy, and quality control tools, (e.g., checklists and templates).
- The outcomes of compliance activities inform the risk assessment (refer to Threat and Risk).
- The compliance process is used to address the findings from the risk assessment (refer to Threat and Risk).



# SeMS at a glance

## Compliance



The following is a non-exhaustive list of indicators that suggest improvement might be needed in your airport's compliance tools and/or mindset:

- There is no internal quality control system in place.
- Poor audit outcomes lead to penalizing of individuals or teams.
- Quality control activities are feared.
- There is no analysis of quality control findings in order to identify root causes of failings.
- Security compliance checks are undertaken by specialists from other parts of the business, (e.g., Safety or Finance).
- The only compliance checks are those undertaken by the TSA.
- Once the site visit component of an audit is undertaken, the activity is deemed complete.
- No follow-up is undertaken to confirm that corrective measures have been implemented and are effective in addressing the identified failing.

The following reflects the change in security mindset, including compliance mindset, after an incident at an airport. Before the incident, airport staff knew that security, and being security-compliant to minimum standards, was important. After the incident, staff moved beyond an intellectual box-checking mindset, to one where they deeply recognized the importance of security processes and behaviors to security outcomes.





# SeMS at a glance

## Protective Security

---

Reducing security risks can be achieved by using non-security-designated resources and security-designated resources.

The focus of this Element is security-designated risk-reduction measures, which include environmental design, physical security measures, and operational security measures.

The protective security measures to be adopted by an airport could be determined by:

- Which measures are most appropriate for reducing the risks (determined by Threat and Risk)
- Compliance requirements (e.g., equipment that is prescribed by regulations)

Protective security is the collection of measures put in place to mitigate security risks (terrorism, protest, and criminality) and meet security compliance requirements. It includes the planning, design, implementation, and operation of those measures. For the purpose of SeMS, protective security relates to those measures that are designed for the purpose of security, (e.g., CCTV and fencing) versus those measures that provide a security outcome but whose purpose is not primarily security, (e.g., speed humps).

### What good looks like

- Protective security is only applied where vulnerabilities cannot be designed out and/or other disciplines, operations, or infrastructure cannot be used to achieve the same security outcome.
- Determining security measures is based on security outcomes, not the purchase of a kit.
- An operational requirements approach is applied to determining protective security needs.
- Physical and operational security are integrated.
- The airport adopts a risk-based approach to design.
- Security equipment is procured based on:
  - User requirements
  - Operational requirements
  - Whole of life costs
  - Consideration of the impact of its implementation on business objectives other than security e.g. passenger experience

For more information about Protective Security refer to Appendix A.







# SeMS at a glance

## Protective Security

The following is a non-exhaustive list of indicators that suggest improvement might be needed in your airport's Protective Security tools and/or mindset:

- There is no reference to the airport's risk assessment when procuring security equipment.
- Security measures are only implemented and reviewed when an instruction from authorities is received.
- Security equipment is procured without consultation with the Security team.
- Infrastructure projects do not involve consulting with the Security team. If they do, it is typically very late in the project and/or only when there is an obvious security scope.
- Protective security measures are implemented in accordance with government instruction only. There is no consideration for finding the same security outcome through other means and/or consideration of how well the protective security measures address the security risks.

### Example

An airport decides to upgrade its terminal to enhance look, feel, and passenger experience. From the first concept meetings, a multidisciplinary group is convened, which includes representation from security experts. Early in discussions, it becomes evident that the very first design proposed would mean a lot of redesign to accommodate CCTV. The architectural and ceiling fixtures designs are revised. In addition, the design team comes forward with some innovative solutions for lighting in some areas, where the passenger aesthetic experience is enhanced, running costs are decreased, and security is improved through the use of automatic lighting in some areas. With the ceiling fixtures and architectural design of the terminal now taking into account the need for lighting and CCTV for security purposes, the need for retrofitting fixtures is removed and integrated Information Communication Technologies is realized. The architectural design reduces the number of lighting and camera fixtures as the CCTV can work more effectively without coverage interference.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



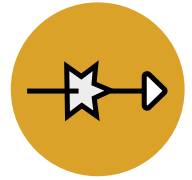
### Example cont.

In contrast, in a different airport, the decision is made to keep the terminal redesign team very small, to be more efficient in making decisions. Concept and high level design are completed quickly, and detailed design and delivery commences. At 80% completion, a member of the security team approaches the design team to ask if he can put the design team in touch with the supplier who will be retrofitting the CCTV cameras. It emerges, in the course of discussion, that the design did not take into account the CCTV field of view and that the lighting provided is inadequate. It is now considered too expensive to undo the work already done. Lighting, which does not fit the design aesthetic, is retrofitted. It is strong, and harsh, and uses up large amounts of energy. Large numbers of CCTV cameras are installed, due to their restricted field of view, and the coverage is still not ideal. The ability to monitor all footage is compromised, and running costs for the cameras and lighting is higher than it would have been otherwise. Passengers also complain about the heat generated from the lights in the summer months, while staff and passengers find the harsh lighting unpleasant.



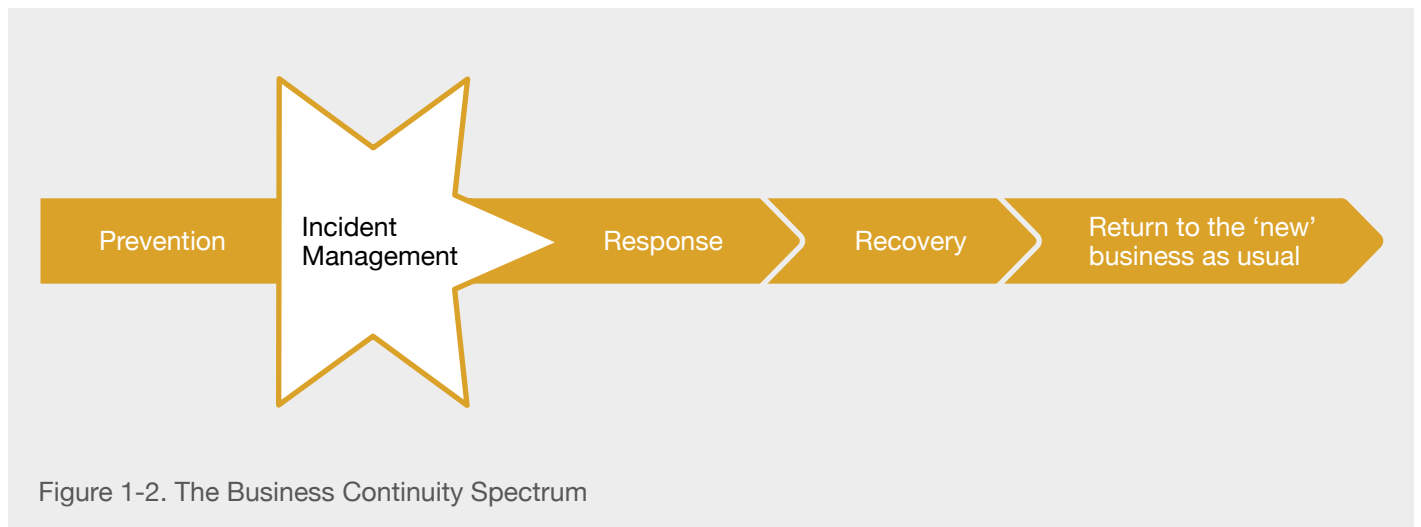
# SeMS at a glance

## Business Continuity, including Incident Management



Business Continuity, including incident management, is about the airport's capability to prevent and prepare for a disruptive event, and to operate at acceptable predefined levels following such an event. The disruptive event may not be security related, but in the context of SeMS, business continuity (see Figure 1-2) is the contribution of security to that capability by way of:

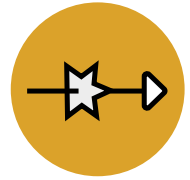
- Preventing a security-related disruptive event (security incident)
- Appropriately and effectively managing the security incident
- Recovering the business post-incident



Ideally, there is a corporate business continuity system in place already in which security is integrated. However, for the purposes of the SeMS the business continuity Element's scope is limited to preventive security, security incident management, and recovery of security operations.

# SeMS at a glance

## Business Continuity, including Incident Management



### What good looks like

- An airport-wide (versus security-specific) Business Continuity System is in place.
- Prevention is based on risk management (see Threat and Risk).
- Preparedness takes into account the entire business, not only security.
- Acceptable levels of operation are agreed upon by all business sectors.
- Response and recovery procedures are practiced and resources are allocated appropriately (e.g., Emergency Operations Center is resourced).
- Personnel are sufficiently knowledgeable and empowered to take action and make decisions during response and recovery regardless of the incident (i.e., they are not bound by scenario-specific response procedures).

The following is a non-exhaustive list of indicators that suggest improvement might be needed in your airport's Business Continuity tools and/or mindset:

- An exercise is considered complete when the site component has finished.
- No follow-up is undertaken to determine if lessons learned have been addressed.
- Your airport does not have a business continuity system in place.
- Key decision makers in the business do not know what to expect in terms of their roles or roles of others in the event of a security incident.





# SeMS at a glance

## Training and Application

---

Training in SeMS knowledge, skills, and the application thereof is an important enabling factor for those who play a part in SeMS implementation and the realization of a positive security culture.

People at all levels of the organization need to be equipped with sufficient and appropriate knowledge and skills, and have the confidence to enact these in a range of situations so that they can contribute to maintaining a secure and healthy workplace. An SeMS requires that a wide range of people, representing the larger airport community, receives training and education on both the SeMS and the role they can play, even informally, in contributing towards enhanced security for the airport.

Training refers to activities undertaken to:

- Raise levels of the airport community’s security management knowledge and skills, in particular, their role in contributing to promoting enhanced security situational awareness and appropriate response
- Provide the opportunity for members of the airport community to develop applied confidence, ability, and desire to apply the knowledge and skills they have learned in real-life situations

The effectiveness of SeMS training should be regularly evaluated, focusing in particular on whether application and development of SeMS is actually occurring as a result of training. This establishes whether it is training or other factors that are actually influencing security outcomes. Application of training refers to the requirement that security knowledge and skills are actually acted upon and put into practice in order for SeMS to be considered effective. In large part, realizing application depends on training that has been designed and delivered to act as a key enabler of behavior change, within a wider security-culture change program.





# SeMS at a glance

## Training and Application

### What good looks like

- Training about security is available to the entire airport community, and not only those with security-designated responsibilities; this is reflected in the Airport Security Training Program.
- A formal security Training Needs Analysis is conducted.
- The effectiveness of training (not just its occurrence) is measured.
- Training design includes principles of behavior change, not only skill and knowledge transfer. This provides for trainees to own and therefore apply with commitment their new skill and knowledge.
- Training content goes beyond process and includes situational awareness and decision making during times of elevated pressure or stress or in non-routine environments.
- Training is delivered using the most appropriate format for the learning, e.g., mentoring on the job, classroom, and shadowing. The practice of applying skills and knowledge is included in the training delivery.
- Training across the airport is integrated so that there is a growth in competence and confidence, building upon existing knowledge. For example, staff receive not just a one-off session when their airport badges are issued, but training is reinforced in day-to-day work such as toolbox talks, staff meetings, awareness campaigns, and performance criteria.

The following is a non-exhaustive list of indicators that suggest improvements might be needed in your airport's Training and Application tools and/or mindset:

- Training is determined by frequency alone.
- The effectiveness of training, i.e., measuring peoples' learning and change in behavior and/or skill application is not undertaken.
- Training is considered to only refer to classroom-based knowledge sessions.
- Training is the only mechanism used to make changes to people's knowledge and behavior.
- Training is not welcomed because it takes people off the job.
- There is no consideration given to Threat and Risk, Continual Improvement, or Compliance when determining what training is needed.

For more information about Training and Application refer to Appendix A.





### Example

A small airport decides that its staff needs training in order to improve security behaviors. They decide to conduct a training-needs analysis (TNA) ahead of some training that they want to roll out. Although the person carrying out the analysis is not an HR or Training expert, she reads up on how to conduct a TNA and fully engages in the activity. She carries out the analysis using one-on-one interviews with people who interact with passengers and customers on a daily basis, observation of staff in the course of their work, a security exercise, a desktop analysis of top customer and passenger concerns and complaints, and a review of the security incidents and near misses reported in the last 2 years.

It becomes clear, upon looking at the results of the analysis, that:

- The passenger screening process generates a lot of passenger dissatisfaction.
- There is overlap between a wider airport campaign of caring for the customer and the principle that security is everyone's responsibility, which is also a way of caring for everyone at the airport, whether staff members or passengers.
- There are people who interact with customers and passengers, but who are not typically considered as needing security training as they do not hold formal security roles.
- Staff are saying that while they know the policies and procedures regarding security well, they do not consider security to be their problem. In particular, their supervisors and managers often send the message that security is in the hands of designated security personnel.
- The staff do not feel confident to enact the procedures they have learned, which is particularly revealed under the stress and pressure of the security exercise.
- A surprise strength is revealed: staff know and like each other very much. For example, they know the regular taxi drivers who drive different shifts, and, where possible, they step in to assist each other beyond their job roles. They often instinctively know when a passenger might be trouble in the queue. They even know who best seems to be able to soothe different personalities of passengers!

As a result, the decision is made to integrate security training into pre-existing customer service training, rather than providing it as a stand-alone.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



### Example cont.

Additional training is made available to a wider network of staff. Instead of long classroom-based training, short slide bursts, or prolonged exercises, the decision is made to run short scenario exercises once a month within teams. Each exercise consists of a 15-minute real-life practice of a security scenario, followed by 15 minutes of feedback and discussion. Teams include the cleaning and maintenance staff, check-in staff, and retailers. Teams are convened around the scenario, not only their functional allocation, to mimic the real life conditions that occur when an incident takes place. Predominantly, the scenarios are designed to help staff develop their situational awareness to cues that something is out of place, and then move to action based on that situational awareness.

After a few months, an evaluation is carried out by running another exercise and holding some interviews. While not highly sophisticated, it finds that:

- There are fewer deficiencies identified by the exercise. While staff may not follow exact procedures, they communicate much better, and seem much more alert to the range of factors to keep in mind in a stressful event.
- Near-miss reporting, as well as informal discussion on security matters, has increased. For example, in noticing a new taxi driver in an unfamiliar car, airport staff take the time to approach and make themselves familiar with them.
- The staff actually seem to enjoy the scenarios, and attendance remains high. They also report feeling more safe and secure in their personal lives, due to the situational awareness they have been putting into practice.
- Staff are making the connection between security and caring for the customer. Passenger complaints have decreased. While it is hard to pinpoint the root cause for this improvement exactly, it seems that staff are more considerate and friendly when engaging in their security duties, which seems to be having a positive influence on the passenger experience.





# SeMS at a glance

## Continual Improvement



Security threats are evolving rapidly, and with that, security risks continually change. In response, an SeMS needs to constantly be one step ahead; what was effective yesterday may no longer be effective today. Continual improvement is the process of continuously assessing, and then putting actions in place to improve:

- Whether you are doing the things you have chosen to do right
- Whether the things you have chosen to do were the right things to do in the first place
- Whether the assumptions you had in place to decide that those were the right things, are in fact right
- The root cause of failings

### What good looks like

- Anyone is prepared and empowered to challenge deep assumptions about the business in the context of improvement.
- A culture and system are in place that encourage innovation, and mistakes are viewed as learning opportunities.
- There is proactive exploration of how security can be integrated into airport operations rather than simply imposing or bolting on security.
- Examination of better security extends beyond security outcomes, but includes other business objectives, e.g., passenger experience, efficiency, and cost management.
- Effectiveness of security measures has a status that is equal to or higher than compliance.
- Feedback loops are included to more effectively assess not only how things have been done, but also the impact of the outcome and what could be done better.
- The focus of quality control activities (e.g., audits) is to resolve deficiencies (versus the site visit associated with the audit).
- Leadership attention is on mitigation of security risks, not looking backward and focusing only on avoiding a repeat of what has gone wrong in the past.
- There is a public policy on security, and C-suite/Executives incorporate security into all their corporate-level discussions and statements.

The following is a non-exhaustive list of indicators that suggest improvement in your airport's Continual Improvement tools and/or mindset might be needed:

- “We have always done it like that,” is often heard.
- No root-cause analysis of deficiencies, failings, or incidents is undertaken.
- Security is only ever discussed by senior management when there is a problem.
- Security improvement is about meeting compliance needs only. Achieving the same or better security outcome more efficiently, with improved passenger experience or less resources is never considered.
- Mistakes are often repeated.
- Quick wins tend to be put in place for improvement, without consideration of possible unintended negative consequences that may result.





# SeMS at a glance

## Leadership and Empowerment

The effectiveness of an SeMS is greatest when first the leadership, and then all members of an organization, commit to and support security as a way to enact their core values. This requires leadership from both above and within the community, supported by an organizational culture that is fair and reasonable. That culture is characterized by people who are motivated to do the right thing, have no fear in pursuing it, and are empowered to do so. The empowerment comes from a combination of desire and motivation within the individual and organizational mechanisms and support, including a blame-free environment.

This ideal model is illustrated in Figure 1-3.

The security culture enables or hampers an organization's Security Management System, and directly influences security performance. A positive security culture must be generated from the top down. It starts with the corporate Security Policy and is built on the principles and actions of management.

International Standard for Business Aircraft Operations (IBAC) – 2012

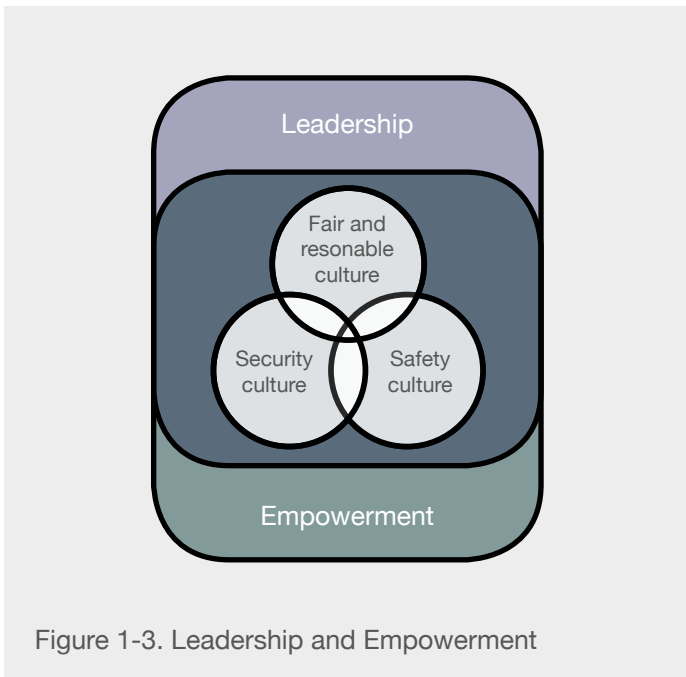


Figure 1-3. Leadership and Empowerment





### What good looks like:

- Senior management places strong emphasis on security as part of the strategy of controlling risks, including minimizing losses.
- Communicating relevant and appropriate security information at all levels of the organization (both within and with outside entities) is valued and actioned.
- Those in senior positions:
  1. Foster a climate in which there is a positive attitude towards criticisms and comments
  2. Value feedback from lower levels of the organization on security
  3. Do not use their influence to force their views on subordinates
  4. Encourage root cause analysis of failings
  5. Implement measures to contain the consequences of identified security deficiencies
- The environment is open to reporting mistakes, which are seen as opportunities to improve.
- A blame-free culture is actioned and not just rhetoric.

The following is a non-exhaustive list of indicators that suggest improvement might be needed in your airport's Leadership and Empowerment tools and/or mindset:

- Security is only considered by the Executives when decisions need to be made about capital equipment purchase, a Security Directive has been issued that requires additional resourcing, or there is a security incident.
- There is no public security policy statement.
- Security is not part of the enterprise risk management framework or system.
- Staff members do not report near-misses, mistakes, security vulnerabilities, or suspicious activity for fear of being penalized.
- Adverse compliance assessment outcomes often result in individuals being blamed.
- Security is seen as purely the domain of senior/Executive leadership, or those with formal security designations.





# SeMS at a glance

## Leadership and Empowerment

### Example

A false alarm, due to miscommunication, has resulted in panic and a chaotic evacuation at the airport. In the process, several people suffered minor physical injuries, and there has been widespread discussion about the unnecessary anxiety caused to passengers, customers, and staff.

In a quickly convened wash-up meeting after the incident, the Head of Security and Head of Operations conducted a root-cause analysis of the incident. The conversation was focused on asking questions such as, “Who was responsible for making the first radio report?”, “Why did the control room operator not immediately notify security?”, and “Why did the security guards on shift not exert better control over the situation?”

The atmosphere in the room was tense and accusatory in tone. For example, when one of the people in the room admitted that he had not followed protocol in the heat of the moment, the Head of Security retorted, “Well, that is simply not good enough, you should have known better – it had better never happen again.” The resulting actions were to put in place more complete process instructions around incident reporting, and to refresh everyone with a half-hour presentation on correct protocols in incident situations.

A different scenario could play out as follows:

A false alarm, due to miscommunication, has resulted in panic and a chaotic evacuation at the airport. In the process, several people suffered minor physical injuries, and there has been widespread discussion about the unnecessary anxiety caused to passengers, customers, and staff.

In a quickly convened wash-up meeting after the incident, the Head of Security and Head of Operations conducted a root-cause analysis of the incident. At the start of the meeting, the Head of Operations asked everyone to relax. He said that the incident had been unpleasant all around, and he recognized that this was not the sort of scenario that anyone would ever wish to see happen in an airport. The proceeding conversation then focused on statements like, “Between us, let’s reconstruct the chain of events that happened, not focusing on who is at fault, or who was responsible, but simply to understand how the incident played out.” Once that exercise was completed, the Head of Security went on to ask questions such as, “What made it difficult to follow the protocol when the incident was first reported?” and “I know we have had training on this, and yet we could not follow it in real life. What assumptions might we be making about how the training is helping us?”

The atmosphere in the room was focused, and was one of curiosity and inquiry. For example, when one of the people in the room admitted that he had not followed protocol in the heat of the moment, the Head of Security responded, “Well, I know it cannot be easy seeing everything that ensued. Let’s see if we can understand the factors that contributed to you not following protocol – talk me through exactly what happened, how you felt, what was going on at the time.”



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices

# SeMS at a glance

## Leadership and Empowerment



### Example cont.

At the end of the session, some fundamental points had been identified as needing attention. Everyone agreed that protocol was very clear; the challenge was carrying it out in real life, in heightened states of anxiety, and the training provided so far was not adequate. It was agreed to carry out a training needs analysis to better identify what exactly could help improvement in a similar situation in the future.

The contrast between these two options is one of leadership and empowerment. In the first instance, an accusatory tone contributed to a session where people were afraid to speak up about the real problems they encountered in this situation. It would have taken a very brave person to step up and challenge back. As a result, nothing fundamentally changed in the security process or protocol, and the airport would have been left in no better position concerning their ability to improve security. Leadership was not role-modeling a genuine concern for security outcomes.

In the second instance, leadership is focusing on fact, not person. The tone is one of inquiry, not blame. There is commitment to working out what exactly happened, and a willingness to challenge assumptions to get to the answer. The result is a team of people who are empowered to speak up, share their experience, and share valuable information. A much better solution then followed.

For more information about Leadership and Empowerment, refer to Appendix A.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# SeMS at a glance

---

## The Elements working as a system

Each Element contributes to improving security outcomes. Their greatest value in contributing to a positive security culture and security being integrated into the fabric of the business is realized when the Elements are seen as working together and with the rest of the airport business.

The following examples illustrate how the SeMS Elements can work together to achieve an improved security outcome:



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# SeMS at a glance

Covert monitoring of employee tailgating through SIDA Control Points

**No SeMS**

Element	Action
Training and Application	Staff are retrained
Compliance	Further covert monitoring
Threat and risk	Further failures result in staff being fired

Consequences/outcomes

- Increased training costs
- Increased recruitment costs
- Increased operating expenses
- No change in security outcome

**With SeMS**

Element	Action
Continual Improvement	Root cause analysis undertaken; identifies that the sole priority is to increase speed to work zone in SIDA area so staff can register on time-clock
Continual Improvement Leadership and Empowerment Compliance	Performance metrics are revised and there is a balance between security and time clock locations so staff can register landside and proceed appropriately through SIDA door
Leadership and Empowerment	New performance metrics are communicated
Compliance	Further covert monitoring
Continual Improvement Leadership and Empowerment Threat and Risk	Improvement in test results are celebrated

Consequences/outcomes

- Improved security outcome
- Reduced vulnerability
- Improved staff morale
- No change in training or recruitment costs



# SeMS at a glance

The following provides examples of how the individual Elements will relate to each other.

The above are simple examples, and the Guidance provides you with other indicators on each

Threat and Risk Business Continuity	Your airport-level threat and risk assessment will identify the threat scenarios that you are most concerned about. This information may inform the exercise schedule you are undertaking for the Business Continuity System.
Protective Security Compliance Threat and Risk	Regulations may dictate what equipment you are required to purchase. Your Threat and Risk assessment, however, may identify risks that the prescribed security equipment will not mitigate (e.g., landside).
Threat and Risk Leadership and Empowerment Training and Application Protective Security	Your Leadership is keen to better understand emerging Threats and Risks. As a result of a study and agreement, you adjust your training program to introduce a new skill set to a select group of personnel, and commence a study into understanding emerging technologies that may be procured in the future to further mitigate the emerging risks.
Training and Application Continual Improvement Threat and Risk	Your security team analyzes the reporting in the confidential reporting system and identifies that there are some worrying trends emerging that point to suspicious activity associated with a number of individuals who work at the airport. The reports are made by non-security personnel. When reported to law enforcement who unknown to you at the time have related intelligence, choose to proactively monitor staff, and it is revealed they are in fact planning an attack on an aircraft facilitated through your airport.

Element's relationship with other Elements. Depending on the maturity of the Element's tools and mindset, the interdependencies will vary. For example, if you are seeking to improve your Leadership and Empowerment, it may be counterproductive to immediately apply punitive action in response to Compliance outcomes. Another example is purchasing security equipment without first understanding what risks you are seeking it to mitigate.



# SeMS at a glance

An SeMS is a mechanism to integrate security into the fabric of the organization. SeMS Elements, either collectively or independently, must interface and integrate with other business operations and mechanisms. The following provides examples of how individual Elements might integrate with other parts of the airport business.

Threat and Risk	Is the security threat and risk assessment an integral element of the airport's enterprise risk management framework?
Compliance	Is the Finance Director involved in reviewing the corrective action plan that is developed following quality control activities?
Protective Security	Consider the use of the CCTV system to support airport operations; can the safety and security patrolling requirements be aligned?
Business Continuity, including Incident Management	Are the regulated emergency response arrangements integrated with the Airport's Business Continuity Management System?
Training and Application	Does the security team have separate human resources, recruitment, and training arrangements, or can security learn from the broader HR initiatives (e.g., talent programs)?
Continual Improvement	Is the airport's insurance company aware of the airport's security culture and the role it plays in reducing risk? Can this provide insurance premium savings?
Leadership and Empowerment	Does the airport's reward and recognition scheme include security?



# Are you SeMS ready?

---

What questions does this section answer for me?

- + To what degree is my airport really ready to take on an SeMS?
- + What is the most appropriate starting point for my airport to begin the SeMS implementation journey?
- + What can I expect to encounter when implementing an SeMS?

Answering these questions means you are more likely to choose a starting point for your airport's SeMS journey that is manageable, and therefore more likely to be achieved.

---

# Assessing your SeMS readiness



To assess your SeMS readiness, ask and answer the following two questions.

## Question 1: How urgently do we want to implement SeMS?

To answer this question, pick just one of the two options below (A or B). There is no right or wrong answer. It is important that you do not choose the answer you would like or that you think is right. Instead, choose the one that most accurately captures the most common thinking that you see/hear/experience when it comes to security at your airport. If the reality is that your airport or organization falls somewhere in the middle, pick the answer you think is the closest match.

Option A:	Option B:
<p>There is a low urgency to implementing an SeMS. The message from leadership is that it is acceptable if it takes us a while. There are other priorities in the airport right now, which means that an SeMS will happen when circumstances allow. Our urgency would increase if there was a formal compliance requirement, or if something occurred (e.g., an incident) that made us re-evaluate the urgency.</p>	<p>There is a high urgency to implementing an SeMS. There is real pressure, whether from leadership, the industry, our customers, our business values, our strategy, or compliance requirements, to see meaningful movement on this issue. There is a willingness to immediately make resources (time, money, and people) available to help move this project along.</p>



# Assessing your SeMS readiness

## Question 2: What do we think an SeMS is?

Choose the Option that might accurately capture the prevalent thinking in your airport. It is important that you do not choose the answer you would like or that you think is right. Instead, choose the one that most accurately captures the most common thinking that you see/hear/experience when it comes to security at your airport. Again, you will not get an answer that exactly matches your airport's thinking. You should choose the one that, all things considered, seems the best fit.

Option 1:	Option 2:
<p>An SeMS is improved through a process approach</p> <ul style="list-style-type: none"><li>• An SeMS consists of a library of policies, procedures, processes, templates, and standards. It is housed in a clear set of documents, which can be tailored to our airport.</li><li>• If we can implement this library, we will be doing well in terms of implementing an SeMS. This is best done through a recurring process of SeMS audit and improvement, against clear standards.</li><li>• The best way to ensure an SeMS is implemented is to appoint clear security specialists, who can make sure the policies, procedures, templates, and standards are put into practice. This frees up other parts of the airport to focus on their core business.</li><li>• Key influencers and decision makers still need to be educated to understand the importance of an SeMS. SeMS experts have to ensure that an SeMS is not forgotten about as airport objectives come first.</li><li>• It would be a good start if we can be comfortable that a standard list of physical security measures (e.g., CCTV, screening, badging, and bollards) are in place according to standards.</li></ul>	<p>An SeMS is improved through a systems approach</p> <ul style="list-style-type: none"><li>• An SeMS is a set of overarching principles that helps us understand how different parts of the organization's operations and stakeholders interact to result in a security culture.</li><li>• SeMS implementation is best initially undertaken as a defined project of business and culture change, where we work out how the whole airport community can collectively adapt to ever-evolving security challenges.</li><li>• The best way to ensure an SeMS is implemented is to use collaborative taskforces, across multiple stakeholders, to collectively develop solutions to security challenges specific to our airport.</li><li>• Key influencers and decision makers see SeMS as an important part of achieving airport values and objectives (e.g., high customer service and cost efficiency).</li><li>• It would be a good start if we can see that we have made progress in connecting together the wider airport community around a common language of what SeMS is, and what good might look like.</li></ul>



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices

# What is your readiness starting point?

Having answered the two questions from the previous section, you are now ready to identify your SeMS readiness state by using the grid below to plot your answers. Each axis corresponds to the two questions asked:

- What is your airport’s urgency on an SeMS? (low or high)
- What is your airport’s definition of what an SeMS is? (process or system)

You can record your results at the SeMS Readiness Worksheet found at Appendix H.

Option 1: SeMS as a process	Option 2: SeMS as a system	
<p>(A1) Watching</p> <ul style="list-style-type: none"> <li>• An SeMS is of some interest to the airport. Interest may not yet have turned into action.</li> <li>• There may be indecision regarding how exactly to drive an SeMS.</li> <li>• There is an expectation for a clearly defined set of standards and documents that explain the exact processes and content to be used to implement an SeMS.</li> </ul>	<p>(A2) Exploring</p> <ul style="list-style-type: none"> <li>• An SeMS might be assumed to be inherently embedded throughout their system already.</li> <li>• There may be pockets of security improvement activity in different parts of the airport that may not yet be joined up.</li> <li>• There may be ongoing conversations about how to intentionally focus on improving security in the airport, without necessarily having set up a specific project or clearly defined set of activities.</li> </ul>	Option A: low urgency
<p>(B1) Doing</p> <ul style="list-style-type: none"> <li>• Likely already implementing SeMS standards, processes, templates, policies, and adopting an established system such as a Safety Management System.</li> <li>• May have an established team that is tasked with implementing an SeMS.</li> <li>• This team could be in the process of putting together, or actively seeking to find, a clearly defined set of documents that explain the exact processes and content to be used to implement an SeMS.</li> </ul>	<p>(B2) Evolving</p> <ul style="list-style-type: none"> <li>• Likely already defining, together with broader airport community, what SeMS looks like as an overarching system.</li> <li>• May have task forces or working groups, or clearly identified individuals or teams, working to co-define an approach to security improvement across the airport.</li> <li>• There may be a number of security initiatives in place, to learn and evolve from, in order to connect different parts of the airport system for enhanced security outcomes.</li> </ul>	Option B: high urgency

# Proceeding with an SeMS



---

Once you have identified your degree of readiness to begin the SeMS implementation process, you can make some decisions on how best to proceed.

The following pages describe the implications of each readiness state, and, in particular, how you should use the rest of this Guidance to best effect.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Proceeding with an SeMS

Readiness level: A1, Watching, low readiness	
Points to note	<ul style="list-style-type: none"><li>• Attempts to proceed immediately with full SeMS implementation will likely fail.</li><li>• Success in introducing an SeMS will be enhanced if a security failure increases a sense of urgency, or if a person or organization in a position of influence mandates its implementation.</li><li>• Be wary of introducing too much, too soon, and risking the development of resistance to future SeMS efforts.</li></ul>
Best way to proceed	<ul style="list-style-type: none"><li>• <b>Your main task is to raise SeMS awareness, and educate your airport, without needing to immediately ask for a full program of change.</b></li><li>• Use this Guidance and the SMAT process described within it to generate early conversations, literacy, and awareness of SeMS.</li><li>• Spend most of your time interacting with different airport stakeholders, and learning what their understanding of SeMS is and what their general security concerns are, before moving into a proposed roll-out of SeMS activities and processes.</li><li>• Consider bringing in technical experts to conduct audits and provide a wider view of SeMS and how it can be beneficial, before trying to ask parts of the airport to commit to action.</li></ul>
Next steps	<ul style="list-style-type: none"><li>• Draw up a list of key stakeholders you want to engage, and meet with them to understand their day-to-day business and their thoughts on security.</li><li>• Turn to pgs. 59, 60 on how to run the SMAT process to generate conversations about security in your airport.</li><li>• Run the SMAT exercise, according to the instructions on pgs. 51-58, 67.</li><li>• Once you have carried out the SMAT exercise and the stakeholder interviews, set up a meeting with the most senior airport leadership you can reach to share and discuss:<ol style="list-style-type: none"><li>1. What you have learned from the SMAT exercise</li><li>2. What you have learned from the stakeholder interview</li><li>3. Examples of how SeMS might contribute to enhanced airport performance</li><li>4. Examples of what happens when SeMS fails</li><li>5. Any metrics you have on the performance of security in your airport, e.g., restricted access breaches</li></ol></li></ul>
What to expect	<ul style="list-style-type: none"><li>• This Guidance is not a pre-set library of processes and procedures. Rather, this Guidance will help you and your airport understand the real drivers underlying SeMS and the system of Elements that makes up SeMS.</li><li>• You can expect some confusion and dissatisfaction that an SeMS is not a clearly articulated list of actions to undertake. This is completely normal.</li><li>• You might spend a lot of time in educational discussions and meetings, simply getting stakeholders aware of and more comfortable with the concept of an SeMS. This is valuable to do and is not wasted time.</li></ul>



# Proceeding with an SeMS

Readiness level: A2, Exploring, low readiness	
Points to note	<ul style="list-style-type: none"><li>• Without an increase in urgency, a development of SeMS governance, and a clear plan for SeMS implementation, there will likely continue to be a lot of interesting discussion with little actual progress on SeMS implementation.</li><li>• Success in introducing an SeMS will be enhanced if a security failure increases sense of urgency, or if a person or organization in a position of influence mandates its implementation.</li><li>• Be wary of stifling an already-receptive environment, where people may already be sharing good ideas to improve an SeMS, by introducing a highly check-listed approach to SeMS.</li></ul>
Best way to proceed	<ul style="list-style-type: none"><li>• <b>Your main task is to help raise the urgency of needing to move beyond thinking to doing something about SeMS. This may mean making the case for urgency, as well as putting in place governance and processes to help turn thoughts and words into reality.</b></li><li>• Consider bringing in technical experts to conduct audits and provide data that might show the urgency for an SeMS.</li><li>• Ensure that, at a minimum, an SeMS Champion and an SeMS Facilitator are identified.</li><li>• Set up an SeMS Taskforce, comprising people from across the airport community who are interested in an SeMS. The SeMS Champion is tasked with ensuring points that can benefit from Senior Airport Leadership decision making are heard, while the SeMS Facilitator tracks items for action and follows up on those items.</li><li>• The SeMS Taskforce can start with the SMAT exercise, described on pgs. 61-65.</li><li>• Once the SMAT exercise has been completed, the SeMS Taskforce can collectively use the decision-making process on pgs. 71-76, 113-114, 138-140 to make recommendations to the Airport Board/Executives.</li></ul>
Next steps	<ul style="list-style-type: none"><li>• Run the SMAT exercise, according to the instructions on pgs. 51-58, 61-65, 67.</li><li>• Use the outputs of the SMAT exercise to inform your SeMS Champion, and to secure senior leadership involvement in putting together an appropriate plan to improve the SeMS in your airport.</li><li>• While the SeMS Facilitator might take on a coordinating role, it is expected that all stakeholders will own actions to improve the SeMS across the airport.</li></ul>
What to expect	<ul style="list-style-type: none"><li>• Use this Guidance, and review of the Elements, to identify where you might be able to generate data to help provide the case for an SeMS.</li><li>• Your main task it to get a group of stakeholders working together, collaboratively, to put in place a structure to help an SeMS mature in an intentional, evidenced, and less haphazard manner.</li><li>• Use this guidance to help you plot out a structured plan and set of activities to help you turn the exploring into action.</li></ul>





# Proceeding with your SeMS

Readiness level: B1, Doing, some readiness	
Points to note	<ul style="list-style-type: none"><li>• There may be a focus on developing libraries of documentation that describe different SeMS processes. This might be occurring without staff having adequately considered the strategic drivers for an SeMS, especially how it contributes to the airport's overall performance and values promises.</li><li>• There may be a reliance on a defined, possibly siloed, group of people to ensure security happens, which could hamper efforts to build SeMS capability within the entire airport system.</li><li>• The SeMS may run the risk of becoming a set of checkbox activities and so become ineffective over time, particularly as security threats and risks are ever-changing.</li></ul>
Best way to proceed	<ul style="list-style-type: none"><li>• <b>Your main task is to ensure that the SeMS becomes systemic in nature, that it becomes everyone's responsibility, and that security activities serve the wider airport interest rather than coming into conflict with other airport functions.</b></li><li>• Set up a clear SeMS Taskforce, comprising people from across the airport community who are interested in SeMS. The SeMS Champion is tasked with ensuring points that can benefit from Senior Airport Leadership decision making are heard, while the SeMS Facilitator tracks items for action and follows up on them.</li><li>• The SeMS Taskforce can start with the SMAT exercise, described on pg. 66. This can assist in broadening understanding of the systemic nature of SeMS, and draw focus to Elements that may not currently be considered in your SeMS activities.</li><li>• Once the SMAT exercise has been completed, the SeMS Taskforce can collectively use the decision-making process on pgs. 71-76, 113-114, 138-140 to make recommendations to the Airport Board/Executives.</li></ul>
Next steps	<ul style="list-style-type: none"><li>• Conduct an SeMS maturity self-assessment using the SMAT (refer to pgs. 51-58, 66, 67).</li><li>• Use the outputs of the SMAT to inform your SeMS Champion, and secure senior leadership involvement in putting together an appropriate plan to improve the SeMS in your airport pgs. 74-77.</li><li>• While the SeMS Facilitator might take on a coordinating role, it is expected that all stakeholders will own actions to improve the SeMS across the airport.</li><li>• Consider bringing in an expert partner who can work alongside your team, tasked with embedding capability within your team to manage the wide participatory behavior change required of airport stakeholders when implementing an SeMS.</li></ul>
What to expect	<ul style="list-style-type: none"><li>• This guidance is aimed at helping airports move maturity levels in terms of SeMS thinking, particularly moving to thinking of the SeMS as an ever-evolving system guided by principles rather than a linear library of processes.</li><li>• You may, then, experience some surprise, or lack of certainty, when starting to undertake activities that include multi-stakeholder working groups, or asking people to interact around principles rather than clearly pre-defined, clear-cut steps and rules.</li></ul>



## Proceeding with an SeMS

Readiness level: B2, Evolving, ready	
Points to note	<ul style="list-style-type: none"><li>• There is likely already a clearly articulated and widely modeled senior leadership commitment to security in the airport, where security is seen as an enabler of airport performance, customer satisfaction, and expression of business values.</li><li>• Airport-wide stakeholders may already be involved in cross-stakeholder security working groups and taskforces (e.g., tenants organizations, airlines, landside, and airside functions).</li><li>• The SeMS may be spoken about and understood as two main themes: (1) as a concept, where security is everyone's business and is best enacted when it is part of everyone's day-to-day behaviors, and (2) a clearly defined project of business or culture change, which might be in progress or has been completed, to put in place a well-managed set of activities to intentionally progress the security culture.</li></ul>
Best way to proceed	<ul style="list-style-type: none"><li>• Periodically conduct a quality assurance review of your SeMS, paying particular attention to ensuring that processes for Continual Improvement are being used to consider questions of security in a proactive manner.</li><li>• Consider sharing your lessons learned and SeMS approach with the wider industry, helping to grow SeMS beyond your airport.</li></ul>
Next steps	<ul style="list-style-type: none"><li>• Conduct an SeMS maturity self-assessment using the SMAT (refer to pgs. 51-58, 66-67)</li><li>• Communicate the outputs of the SMAT, including recommendations, with the Board/ Executives.</li><li>• Consider bringing in fresh eyes, e.g., an external auditor or assurance, to continue to grow, improve, and challenge your approach.</li></ul>
What to expect	<ul style="list-style-type: none"><li>• This Guidance may provide a slightly more holistic approach to your current SeMS practice.</li><li>• You may find some details or suggestions that help refine and mature your current thinking on your SeMS.</li><li>• You may find that you have a well-developed suite of supporting materials that this Guidance does not provide. These materials may have been specifically developed for your airport.</li></ul>



Are you SeMS ready?

## Now you know your SeMS readiness, what next?



---

Now that you have a high-level understanding of your airport's SeMS readiness, you can begin the process of using the rest of this Guidance most effectively.

The next section introduces a series of steps that help you measure your airport's current SeMS maturity, identify gaps where improvement is required, decide how you would like to close those gaps, and then put in place governance and processes to help you keep progressing your SeMS maturity.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# How to Establish your SeMS

---

What questions does this section answer for me?

- + Now that I know how ready my airport is to implement an SeMS, how do I begin?
- + How do I identify gaps in our SeMS and then know what to do to close those gaps?
- + What needs to happen in order to make sure we keep progressing the SeMS in our particular airport?

Answering these questions means you will have a list of activities to carry out that will help you develop an 'as is' picture of your airport's current SeMS, a 'to be' picture of where you would like to go, and a plan of how to get there.

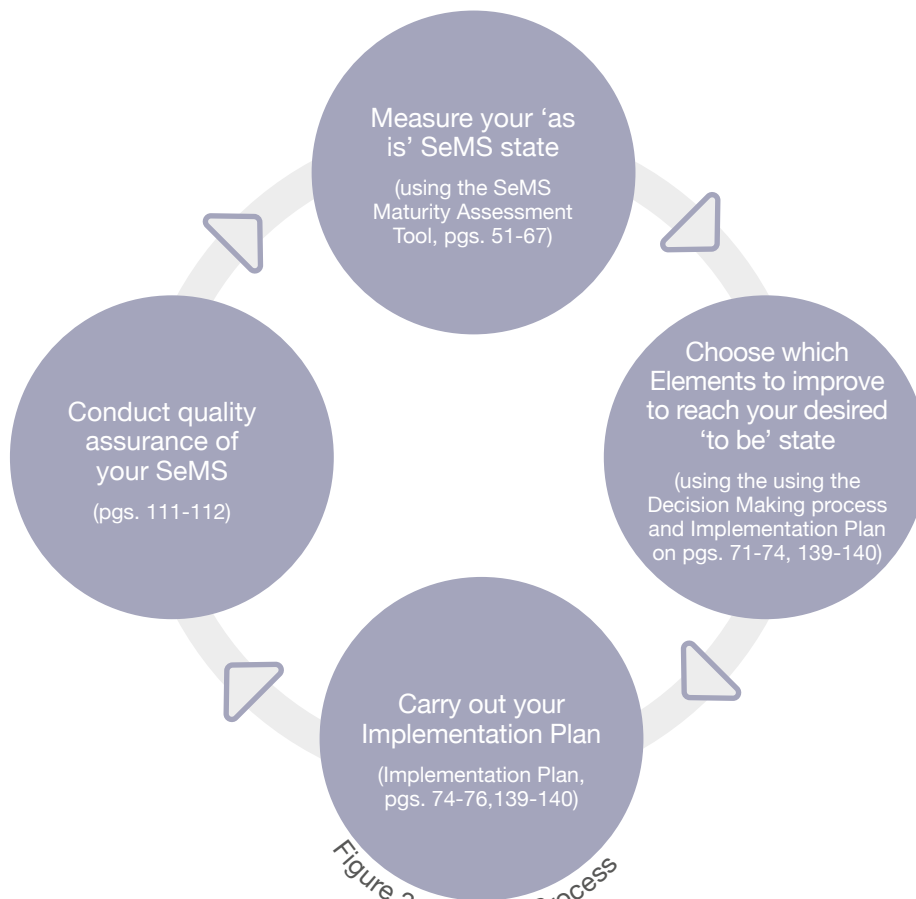
---

# Introduction to how to establish your SeMS

Once the decision is made to establish an SeMS, the SeMS Facilitator will:

- Measure the current 'as is' SeMS state; this is done by using the SeMS maturity self-assessment tool pgs. 55-67
- Choose and prioritize which Elements you wish to mature to reach a desired 'to be' or ideal SeMS state pgs. 71-74
- Implement the guidance to achieve that maturity pgs. 74-76
- Conduct quality assurance on your SeMS pgs. 111-112

To establish SeMS, follow the process in Figure 3-1 below.



# What is the SMAT?

The SeMS Maturity Assessment Tool (SMAT) is a Microsoft Excel spreadsheet containing questions that, once scored, generate a graph to describe the maturity of each Element’s tools and mindset, plus the maturity of the quality assurance of your SeMS.

The process of completing the SMAT, the graphical output it generates, and the discussions and decisions that follow all assist you to:

- 1 Understand what your SeMS maturity looks like today
- 2 Establish a starting point and plan of action to improve your SeMS
- 3 Educate and involve others in your airport’s SeMS

Use the results from the SeMS Readiness exercise (Section 2.2, pg. 41) to determine how you will use the SMAT. The table below shows different ways of using the SMAT, depending on your SeMS readiness level.

Readiness level (pgs. 39-41,137)	Using the SMAT
Watching, low SeMS readiness	<ul style="list-style-type: none"> <li>You will use the SMAT to start generating conversations and introduce the idea of an SeMS.</li> </ul>
Exploring, some SeMS readiness	<ul style="list-style-type: none"> <li>You will use the SMAT to help build a case for action, and create structure and priorities for action.</li> </ul>
Doing, some SeMS readiness	<ul style="list-style-type: none"> <li>You will use the SMAT to make sure that, as you go about implementation, you are thinking about your SeMS as a system, and you are taking into account all Elements.</li> </ul>
Evolving, SeMS ready	<ul style="list-style-type: none"> <li>You will use the SMAT to maintain SeMS, challenge your thinking, and continuously improve your approach.</li> </ul>

The rest of this section describes what the tool measures, and gives different ways of using the tool depending on your readiness level and reasons for carrying out the SMAT.

# What is the SMAT?

---

## What the SMAT measures

The SMAT is premised on the understanding that an SeMS is made up of seven Elements, each comprising tools and mindset. For an SeMS to work well (i.e., be considered mature), the airport needs to ensure that:

- On its own, each Element is working well, including both the tools and mindset.
- All the Elements are working well together, as a system.

The SMAT measures your SeMS Maturity by:

- Asking a set of questions for each Element; the answers to those questions help give an estimation of the maturity of the tools and mindset for each Element
- Generating a graph that shows the maturity of each Element's tools and mindset

## Once the SMAT is completed, what happens next?

Once you have completed the SMAT, you then decide

- Which Elements you want to mature further and prioritize those Elements
- Whether the tools, mindset, or both need maturing in order for the entire Element to progress
- Actions that need to be taken to mature those Elements
- Methods to store and handle the SMAT results appropriately

This section provides guidance on those steps.

## What to expect from the SMAT

The SMAT will provide you with

- A holistic view of all Elements that make up the SeMS system
- An indication of the maturity of each Element's tools and mindset
- An indication of which Elements in your airport need improvement
- A way to get different stakeholders in the airport talking and thinking about what comprises an SeMS
- A way to measure your progress as you implement and maintain your SeMS

You are encouraged to use the SMAT on a periodic basis (e.g., yearly) in order to identify any changes. This activity may form part of the quality assurance of the SeMS itself.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## What is the SMAT?

---

### What the SMAT is not

- The SMAT is not an absolute formula. Airports are complex, especially when considering the wider community of stakeholders. Therefore, the SMAT does not provide a single overarching statement, percentage, or score to state how your airport is performing as a whole when it comes to SeMS. To do so accurately would require a thorough diagnostic process, which could take weeks or even months and is beyond the scope of this Guidance.
- The SMAT is not an exhaustive list of every single process, template, item, or tool that might be used for security, or otherwise, in your airport. The SMAT considers an SeMS as a system of interconnected Elements, and provides you with a way of thinking about each of them systematically.

### Who do I involve when completing the SMAT?

The tables on the next two pages will help you think about whether you might want to have the SMAT completed by individuals, by groups, or a mixture of both.

Each person and/or group completing the SMAT will complete it from their own viewpoint. This means that you might get quite different SMAT results, depending on who completes the SMAT. This is not a bad thing, and is not a reason to pick who completes the SMAT based on who you think will give the most favorable results, or who you think will agree with your perspectives.

What is more important is that differences in perspective, which show up in SMAT results, are shared and discussed. This is a valuable way of recognizing that establishing an SeMS is a group effort, conducted over time, in order to create consistency of experience across the airport.

It can be beneficial to ask a wide range of people who might have quite different perspectives to complete the SMAT. This helps to challenge any assumptions that might be in place regarding how well SeMS is understood and embedded throughout the airport. For example, it might help leadership recognize that Elements that may seem very obvious to them are not as obvious to others.





# What is the SMAT?

Who do I involve?	Why might you do this?	Pros	Cons
<p><b>Completing the SMAT individually</b></p> <p>(Instructions on pgs. 59-60)</p> <p>Consider including:</p> <ul style="list-style-type: none"> <li>• Your head of security</li> <li>• An Executive member</li> <li>• Key people you wish to raise awareness with, e.g., tenant organizations and heads of functions from other parts of the business</li> <li>• Key informal influencers within your system</li> </ul>	<p>It is a good opportunity to get key individuals thinking about your SeMS and generate buy-in prior to asking for more tangible SeMS change.</p> <p>Consider this option in particular if you have decided that your SeMS is in the Watching SeMS readiness state (see Section 2).</p>	<p>You immediately, in a short space of time, have a graph and way to structure thinking about SeMS.</p> <p>If several individuals compare their SeMS outputs, it gives an opportunity for people to start to gain a deeper understanding of different perspectives and experience of your SeMS.</p> <p>The simple act of completing the questionnaire is in itself an awareness-generating experience.</p>	<p>Using a single person’s perspective to generate the SMAT limits the degree to which SMAT outputs can be generalized across the airport.</p> <p>When sharing the SMAT outputs, you might face resistance and challenges to how you reached your conclusions based on a single perspective.</p> <p>At this stage, you may wish simply to use the exercise as an awareness-generating activity, and not put as much focus on agreeing to tangible actions.</p>
<p><b>Completing the SMAT as a group</b></p> <p>(Instructions on pgs. 61-65)</p> <p>Consider a range of people, to cross boundaries within your airport.</p> <p>You might want to invite some senior people, e.g., Head of Security, as well as people who are more involved in day-to-day operations, such as someone from the cleaning and maintenance department, or someone from a tenant organization.</p>	<p>It is a good opportunity to get people talking, in detail, about the SeMS Elements. This helps to start to form a systemic understanding of how an SeMS works, across a collective of people.</p> <p>Consider this option in particular if you have decided that your SeMS is in the Exploring or Doing SeMS readiness states (see Section 2).</p>	<p>People in the group gain a deeper understanding of different perspectives and experiences of the SeMS Elements.</p> <p>People in the group start to generate a shared language around the SeMS, making it easier for them to understand ways to improve it in the future.</p> <p>People start to understand what will be required, collectively, to bring about change to the SeMS system.</p>	<p>This can take some time, e.g., at least a day, if not two, per group.</p> <p>This needs skilled facilitation and time management to ensure the conversation remains constructive, rather than simply debating who is right and who is wrong.</p>



## What is the SMAT?

Who do I involve?	Why might you do this?	Pros	Cons
<p><b>Completing the SMAT with multiple individuals and/or groups and collating the responses</b></p> <p>(Instructions on pg. 66)</p> <p>Consider a wide range of people across levels, functions, and organizations within your airport.</p>	<p>This can be useful when trying to deeply understand the SeMS system and culture across the airport community. It is most beneficial when the intention is to build a clear plan of work that spans the entire SeMS system and airport community.</p> <p>Consider this option in particular if you have decided that your SeMS is in the Evolving readiness state (see Section 2).</p>	<p>You can identify different areas of need in different stakeholder groups and so tailor plans accordingly.</p> <p>You can identify potential areas of opportunity for different stakeholder groups to learn from each other or work together.</p> <p>You can get a good picture of how your SeMS is working across the entire airport system, and prioritize areas for actions that are most needed.</p>	<p>This exercise will take a lot of time to complete, e.g., several weeks or months.</p> <p>With the large amount of information, presenting it in a way that is relevant and useful will require some thinking and development time.</p> <p>If trust between stakeholders is low, you may need to be careful of sharing information that might make a group look bad.</p> <p>It may be better to keep results anonymous. This version should only be carried out if the different stakeholder groups are brought into the process and a non-punitive approach is taken to areas where development is needed.</p>



# How do I use the SMAT?

## Understanding how to make the most out of the SMAT

Before proceeding to the SMAT (the Microsoft Excel spreadsheet titled SeMS Maturity Self Assessment Tool), it is important to read through and fully understand what is expected from the SMAT input, and what you might expect during the process of completing the SMAT.

### What the SMAT will ask you to do

The SMAT is intuitive and is made up of two worksheets:

- 1 The SMAT itself. This starts with some information about you (e.g., name and email), followed by approximately 50 questions/statements. It is your answers to these questions that will inform the maturity of the Elements that make up an SeMS. The questionnaire is based on statements with 3-4 descriptors, from which you should choose one that most closely resembles/describes your airport today – see Figure 3-2 below for an example.
- 2 The SMAT Results (refer to pgs. 56, 68-70, 138)

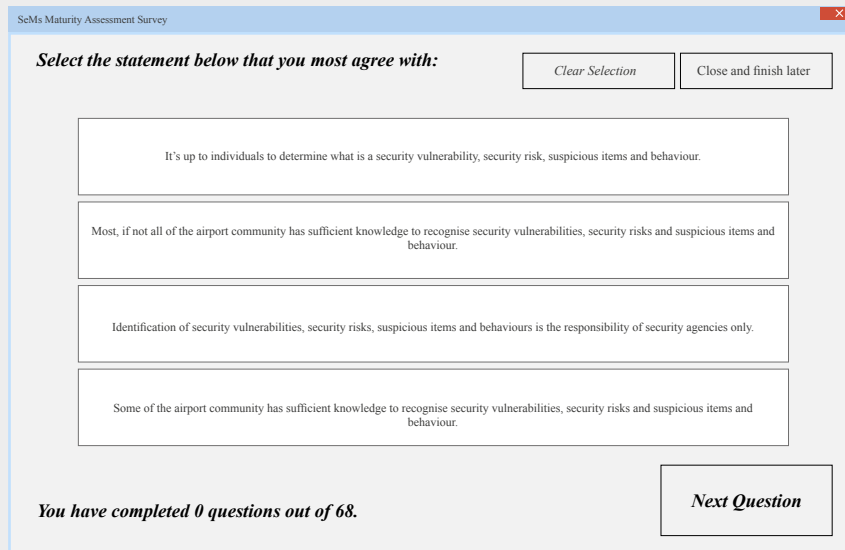
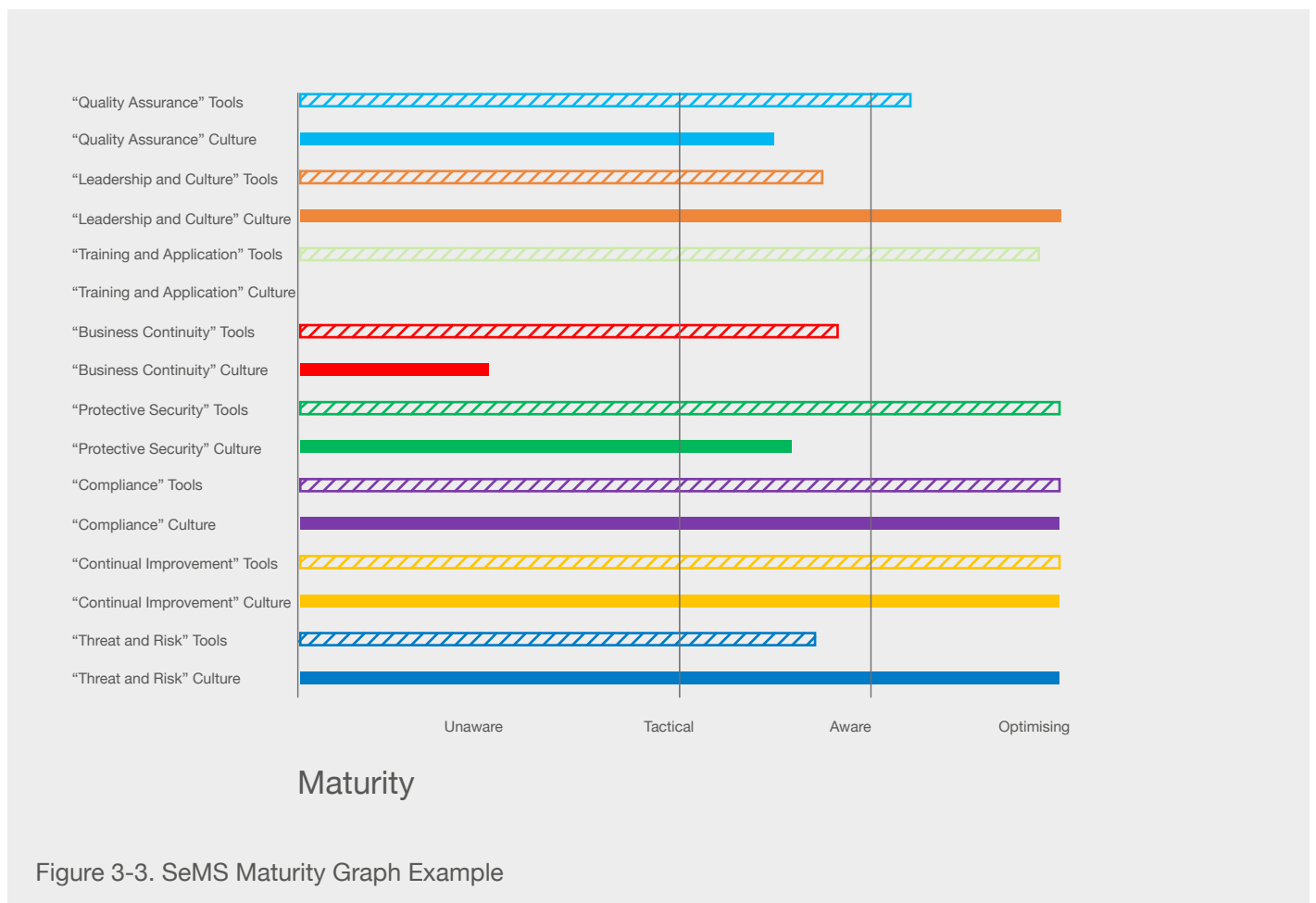


Figure 3-2. SMAT Question Example



# How do I use the SMAT?

Once all the statements in the SMAT have been answered, a graph is generated (see Figure 3-3) within the same spreadsheet that shows the maturity of each SeMS Element's tools and mindset, according to the answers that have been provided. This will be the second worksheet you interact with (you will only be able to read and print it). The graph format (i.e., spider diagram or column graph) will depend on which Excel version you are using.



## How do I use the SMAT?

---

### What should I take into consideration before starting the SMAT?

*Important Note:* It is critical that you respond to each statement honestly so that you know today's maturity. Choosing those descriptors that describe what you would prefer your airport to be like will in fact undermine your efforts to achieve it; you will not have an understanding of where you are today, where you want to be, and what you need to do to get there.

Choose only one option – the one that best describes your airport today. It is tempting to answer in a wishful thinking way, or in a 'what we hope we are' way, but this will provide inaccurate scores and will be less valuable at the end.

There are very subtle differences in the questions, so at times it may feel like you are repeating your answers or have answered certain questions already; however the SMAT is designed to assess your security maturity across a range of levels and contexts.

Before starting the SMAT, it is important to understand that this is not a quick fix or short satisfaction survey and will take a fair deal of time to effectively go through all questions. The SMAT is designed so that you can save your input and come back to it later.

There is value in involving a number of people when completing the SMAT. Involving a number of people reduces the influence of bias and is likely to be a closer representation of the airport rather than individuals' perceptions. Further guidance is provided in the following section, 'Completing your SMAT as a Group'.

This will ensure that the scores from the SMAT will be more accurate and reflective of your organization, and thus you will gain far more value from the recommendations and action steps to take once you have your score.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## How do I use the SMAT?

---

Now you are ready to complete your SMAT. Please refer to the separate SeMS Maturity Assessment Tool (SMAT). Remember, it is better to consult widely and take your time to give considered responses than it is to rush through the SMAT. You can save your SMAT at any time and return to it.

Once you have completed your SMAT, continue to the next chapter for guidance on interpreting the results and next steps.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Different ways to complete the SMAT

---

## Completing your SMAT as or with individuals

### Decide why you want to complete your SMAT as or with individuals

Reasons might be:

- You want to first be sure that you understand the SMAT and how it works, and so be able to better instruct others how to use it and gain benefit from it.
- You are not ready to facilitate a group of people coming to consensus decisions for a group exercise. You may not have the time for this, or feel comfortable enough yet to run a valuable group session.
- You might feel you can gain buy-in from key people if they first do the SMAT as individuals. They are more likely to be completely honest in their input and will be in a better position to champion an SeMS within the airport once they have been through their own individual process of engaging with the SMAT.
- You might have decided that your airport is at the Watching SeMS readiness stage (Section 2).

### Decide who you want to ask to complete SMAT

It might be:

- Just yourself, for now
- Key individuals within senior leadership positions
- Individuals within your team
- Individuals in other teams or in other airport stakeholder groups, who might not normally be asked to think about an SeMS

### Decide how and where you want to go about having the SMAT completed

It might be:

- You, and only you
- You, sitting with someone while they complete the SMAT, guiding them through the questions and instructions
- Asking someone to complete it quietly for themselves, on their own
- A group of individuals, in a room, all completing it individually at the same time
- You, or someone else, gradually completing it in stages over a few weeks

### Decide on the process, or flow, of SMAT completion

The process flow chart on the next page describes the high-level process to follow. The table that follows describes each step in more detail.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

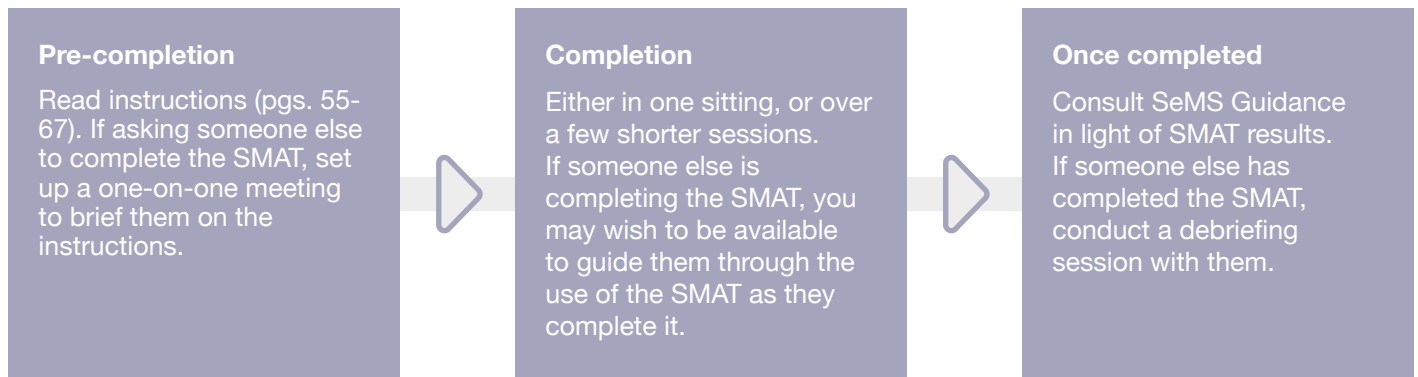
3

How to establish  
your SeMS

4

Appendices

## Different ways to complete the SMAT



<b>Pre-completion</b>	You should read the instructions on pgs. 55-57, 67. If you are asking someone else to complete the SMAT, ensure you have a one-on-one conversation with that person to make sure they understand the mindset required.
<b>During completion</b>	You can complete the SMAT in one sitting, or you can pause and come back to it over a few weeks.
<b>Once completed</b>	Take time to reflect on the results, and to consult the rest of this Guidance document to think about what to do next. If someone else has completed the SMAT, take time to discuss with them what they learned, what questions they have, and what they think they might want to do next.





# Different ways to complete the SMAT

---

## Completing your SMAT as a group

### Decide why you want to complete your SMAT as a group

Reasons might be:

- To use the exercise to help enhance SeMS awareness and understanding in a particular group of people
- To use the exercise to get a more holistic, objective, and accurate view of the current state of the SeMS
- To use the exercise to help groups of people, who may not normally interact on the question of SeMS, see their shared views, challenges, and potential benefits in the implementation of an SeMS
- To use the exercise to gain buy-in and create urgency from a particular group of stakeholders so that they better champion an SeMS
- You might have decided that your airport is at the Exploring or Doing SeMS readiness stages (Section 2)

There may be other reasons, but be sure to focus on the outcome you are looking for (e.g., changing awareness levels) rather than the activities you want to focus on (e.g., telling people about the SeMS).

### Decide who you want to run the SMAT session with

Your reasons for running the exercise (see section above) will help you think about who to invite.

For example, if you are needing buy-in and stakeholder support, are there some people who you could invite who you did not initially think of? Or, if you are wanting champions for an SeMS, are you inviting people who may have influence in an SeMS, even if they might currently be slightly resistant to or unaware of the concept of an SeMS?

Groupings you may consider:

- Leadership and C-Suite
- Multi-stakeholder group; representatives of people who hold formal and informal security roles, as well as those who currently have no involvement in the SeMS at all
- Mix of airport stakeholder representatives (e.g., tenant representatives, airline representatives, ground handlers, and support services)

### Decide how you want to run the SMAT session

Think about the tone or atmosphere of your session. In most cases, and in pursuit of just-culture principles, the tone should be one where everyone gets a chance to share their views. Agreement of views is not to be immediately forced. Time is taken to share with the group what the purpose of the session is (which you can adapt from the 'why'), and for the group to meet each other and set up a positive atmosphere.



## Different ways to complete the SMAT

Think about who is best to introduce the session (perhaps you want someone senior to set the scene e.g., SeMS Champion, even if they are not there for the rest of the session), and who is best to actually run the session (e.g., someone familiar with your SeMS, or someone with a facilitation style that is favorable to running open knowledge-sharing sessions).

### Decide where you want to run the SMAT session

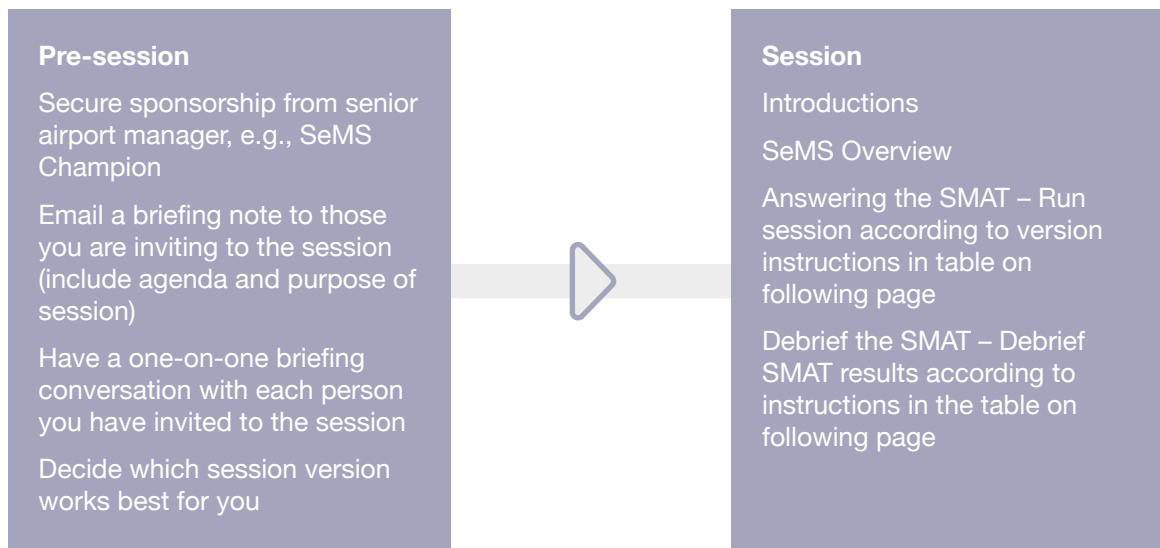
You will need somewhere big enough to accommodate everyone, preferably with space for people to work together in clusters or smaller groups, as well as in bigger group discussions. You will need somewhere to plug in at least one laptop and a projector screen. Flip charts are preferable, though not absolute necessities.

If you are inviting people from groups who do not often get invited to security discussions, consider whether you want to use a venue that is more convenient for them (rather than your usual meeting rooms).

### Decide on the process, or flow, of the session

A suggested outline agenda is provided below, but you will adapt this depending on how many people are attending your session, how much time you have available, and what purpose or 'why' you are trying to achieve by using the SMAT. The result of your SeMS readiness assessment will answer the 'why'.

The flow chart below describes the high-level process. The table that follows describes each step in more detail.



## Different ways to complete the SMAT

<b>Pre-session</b>	<ul style="list-style-type: none"><li>• Gain agreement from someone senior in the airport, to give their sponsorship to you running this session. This may be facilitated by the SeMS Champion.</li><li>• Send an email to the people you have decided to invite, explaining the purpose of the session, what their contribution will be, and the timings of the session. To highlight the importance of the SeMS, the SeMS Champion may do this or provide supporting communication.</li><li>• Take time to have a quick phone call with persons you have invited, to help them understand further why they are invited and what they will be asked to do (often an email is not enough!)</li></ul>
<b>Session</b>  (Depending on how you run it, allow between 3.5 hours and an entire day for the session)	<b>Introductions</b> <ul style="list-style-type: none"><li>• Introduce yourself and your role (you might ask your Champion to do this) (10 mins).</li><li>• Recap why you have asked people to be here today, and that you are going to be asking them to provide their answers to a range of questions designed to help understand the maturity of the airport's SeMS (10 mins).</li><li>• Recap how you would like people to interact with each other today – no blame, no judgment, and open sharing of perceptions and experiences (which may not always be in agreement) (5 mins).</li><li>• Give people an opportunity to introduce themselves, their roles, their level of familiarity with SeMS (and it's ok to say, "I don't know anything about SeMS"), and what they think of when they hear the word security. Depending on how many people are present, you can ask each person in the room, or divide them into smaller groups of 3 or 4 (allow 3 minutes sharing per person, with an additional 5 minutes for general discussion).</li></ul> <b>SeMS overview</b> <ul style="list-style-type: none"><li>• Introduce people to the Elements of SeMS (very high level, 10 mins).</li><li>• Introduce people to a summarized version of pgs. 55-57, 67, including the need for honesty when providing answers to the questions (10 mins).</li></ul> <b>Answering the SMAT</b> <p><i>Answering the SMAT – Version 1</i></p> <ul style="list-style-type: none"><li>• Either as one group or several clusters of smaller groups, pose each SMAT question, one by one.</li><li>• For each SMAT question, each person in the group indicates what their personal answer would be. It is important that people are completely honest in their contributions. Depending on how much time you have, you can ask people to simply give an answer (should take a second or two per person), or else give their answer with a reason (could take up to a minute per person).</li><li>• The most frequent answer is the one that gets inputted in to the SMAT. If there is a tie, allow a further 2 minutes for the group to decide what the final answer is.</li><li>• This exercise, answering all questions on the SMAT, will take 2–3 hours.</li></ul>



## Different ways to complete the SMAT

### Session cont.

(Depending on how you run it, allow between 3.5 hours and an entire day for the session)

### Answering the SMAT – Version 2

- Either as a group or several clusters of smaller groups, pose each SMAT question one by one.
- On a rotating basis, only one person in the group selects an answer to the question. This answer is inputted without challenge, unless someone in the group has a particularly strong objection.
- This version of the exercise will be much quicker (approximately 1.5 hours), but will be less robust in terms of challenge.

### Answering the SMAT – Version 3

- Have several small groups (e.g., 1s, 2s, or 3s, each with their own laptop) complete the SMAT over the course of 1.5 hours.

### Debriefing the SMAT

- Ask each participant to share how they found the experience of completing the SMAT. Was there anything unexpected in the questions, something that surprised them, something they had not thought of before? (Allow 3 minutes per person, or allow small group discussion for 5 minutes and then give a further 10 minutes for plenary group sharing.)
- If you used *Answering the SMAT – Version 1* or *Version 2*, show the entire group the SMAT outputs. Ask them what stands out for them—what is expected, what is unexpected? (Allow approximately 10 minutes for this.)
- If you used *Answering the SMAT – Version 3*, allow groups to look at the SMAT outputs for each group and compare and contrast results, as well as reasons for similarities or differences (allow 20 minutes for this).
- Agree with the group about next steps, in light of the SMAT outputs. Options might be (allow 20 minutes for this):
  - Reconvene to collectively decide improvement areas to focus on.
  - Hold some further one-on-one discussions, to further refine understanding, before finally deciding final SMAT outputs.
  - Ask each delegate to commit to one thing, to help raise awareness of the SeMS, or take a step towards improving the SeMS.

### Close

- Clarify next steps, even if you only decide what you are going to do next after this session.
- Thank the group for their participation.
- Reiterate any outputs that you have agreed to capture and share with the group.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Different ways to complete the SMAT

### Options

You could run versions of this workshop over several shorter sessions. For example, you might run the SeMS overview, ask groups to go and complete the SMAT on their own time, and then bring groups back to debrief the outputs.

Or, you may choose certain sections of the SMAT to focus on, or you might populate some areas that you feel confident on, and ask only for input on those questions where you feel less confident (although, beware of personal bias creeping in).



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Different ways to complete the SMAT

---

## Collating SMAT results across individuals and groups

### Decide why you want to complete your SMAT as a collation across individuals and groups

You may want to:

- Form as much of a complete picture as you can of SeMS across the wider airport community.
- Help the airport stakeholders (e.g., Board, Executives, or different airport organizations) get a big-picture understanding of SeMS across different parts of the airport system.
- Put together a coherent plan for SeMS across the entire airport system, which will be informed by the SMAT results.
- You might have decided that your airport is at the Evolving readiness stage (Section 2).

### Decide who is going to complete the SMAT, and how and where they are going to complete it

Options include:

- You can bring together many teams, each team coming together in a group workshop (pgs. 61-65), to generate a SMAT per group. For example, with the security team as a group, senior leadership as a group, or each different tenant organization as its own group.
- You might ask several individuals to complete the SMAT independently (pgs. 59-60).
- You might have a mixture of both group-completed SMATs and individual-completed SMATs pg.66.

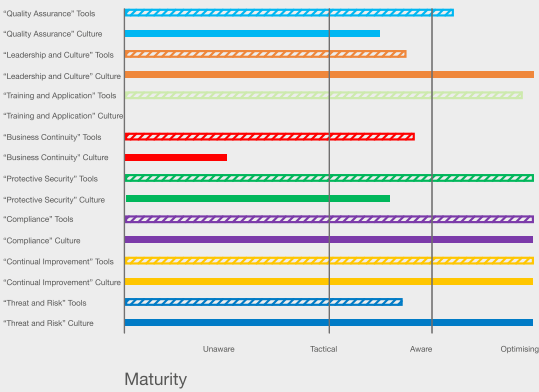
Remember, it is important to emphasize that SMAT completion is about learning, and should not be carried out in a punitive environment. To allow open and honest sharing, it might be necessary to keep contributions anonymous.

### Decide on the process, or flow, of SMAT collation and feedback

The process flow chart below describes the high-level process to follow. The table that follows describes each step in more detail.



# Different ways to complete the SMAT

<p><b>Pre-SMAT completion</b></p>	<p>Explain to each individual or group what you are doing and why. Emphasize that this is about learning together.</p> <p>Ensure that you have a clear plan of how you are going to have the SMATs completed (e.g., a series of group workshops).</p>
<p><b>During SMAT completion</b></p>	<p>Follow the instructions for individual (pgs. 59-60) and group (pgs. 61-65) SMAT completion.</p>
<p><b>Once the SMATs are completed</b></p>	<p>Decide how you want to represent the SMAT outputs. You may want to show the results in a bar graph per Element, for example:</p>  <p>While it may be tempting to work out averages, we do not encourage this approach. Differences between groups get lost, and it is the nuance and difference between groups that is most useful to understanding SeMS accurately across the airport.</p>
<p><b>Share the results</b></p>	<p>Ensure that you give feedback to those who participated in the exercise, even if you show only high level anonymized outputs.</p>

## Storage and Handling of the SMAT Results

While the SMAT results are not Sensitive Security Information (SSI) as defined by 49 CFR part 1520, they could highlight where potential vulnerabilities may be in your airport’s security system. This information may be of interest to individuals who have intent to undertake or facilitate an act of unlawful interference. This should be considered when storing and handling the SMAT results. You should refer to your airport’s policy on handling information that may be considered sensitive or follow the TSA’s SSI Best Practices Guide for Non-DHS Employees and Contractors.

# Interpreting your SMAT results

Now you have completed your SMAT you will know the maturity of:

- The tools and mindset of each of the seven Elements
- The quality assurance of your SeMS

## What Element maturity means

On your SMAT results, you will see a graph that shows the maturity level for each SeMS Element.

The maturity levels can be described in general as follows:

<p><b>UNAWARE</b></p> <p>Tools and culture (almost) do not exist coupled with ‘no desire’ to change.</p>	<p>Typically, the application of security is limited to those individuals with designated security responsibilities. Attitudes towards security is hostile or at best dismissive. Security is not a valued function within the airport. The quality of the security application is likely to be poor.</p>
<p><b>TACTICAL</b></p> <p>There is evidence that some tools and required culture exist.</p>	<p>Typically some but not all tools have been developed. They may be used intermittently but are not considered to be an integral part of the business. People know security is important but do not proactively engage or understand their role. It may be that the catalyst for security efforts are regulatory audits and effort will be made to prepare for those audits. Apart from the audit related effort, there will be little to no effort made to improve security.</p>
<p><b>AWARE</b></p> <p>Tools and required culture exist but utilization and value is not an integral part of the airport community.</p>	<p>Typically security is widely acknowledged as a valuable function within the airport. There will be pockets of positive and proactive security culture. Tools are widely used but the outputs are not necessarily integrated with the rest of the business, for example, a risk assessment matrix is used by the Security Team to inform the application of security measures but it is not utilized in capital investment projects to inform the design or by Finance to inform annual budgets.</p>
<p><b>OPTIMIZING</b></p> <p>Tools and culture are lived as part of the daily fabric of the airport’s operations.</p>	<p>Security is an integral part of the airport’s business. There is a common understanding of its value throughout the community from Executive through to tenant staffs. Every member of the airport community behaves in a way that demonstrates they know they are contributing to the airport’s security. The SeMS tools inform and are informed by non-security business units, for example, a threat and risk assessment is a key basis of design for capital investment projects, regardless of the project’s scope.</p>





# Interpreting your SMAT results

Remember, the SMAT does not give a single overall score for SeMS maturity. This is because the SMAT assesses the maturity of each Element’s tools and mindset, and each has a different influence on your SeMS. The systemic nature of SeMS means that changes in one Element’s maturity will have flow-on effects on others. For example, most of your Element’s tools and mindsets may be close to or at Optimizing; however, if you have one Element that is Unaware, the entire system is less mature—this influence is not shown in individual scores. It is best to use the SMAT to understand how to prioritize your efforts for improvement (i.e., which Element tools and/or mindset) to improve the overall system’s effectiveness.

## Where you are today

The SeMS output graph will look similar to Figure 3-4 below (the scores will be unique to your airport):

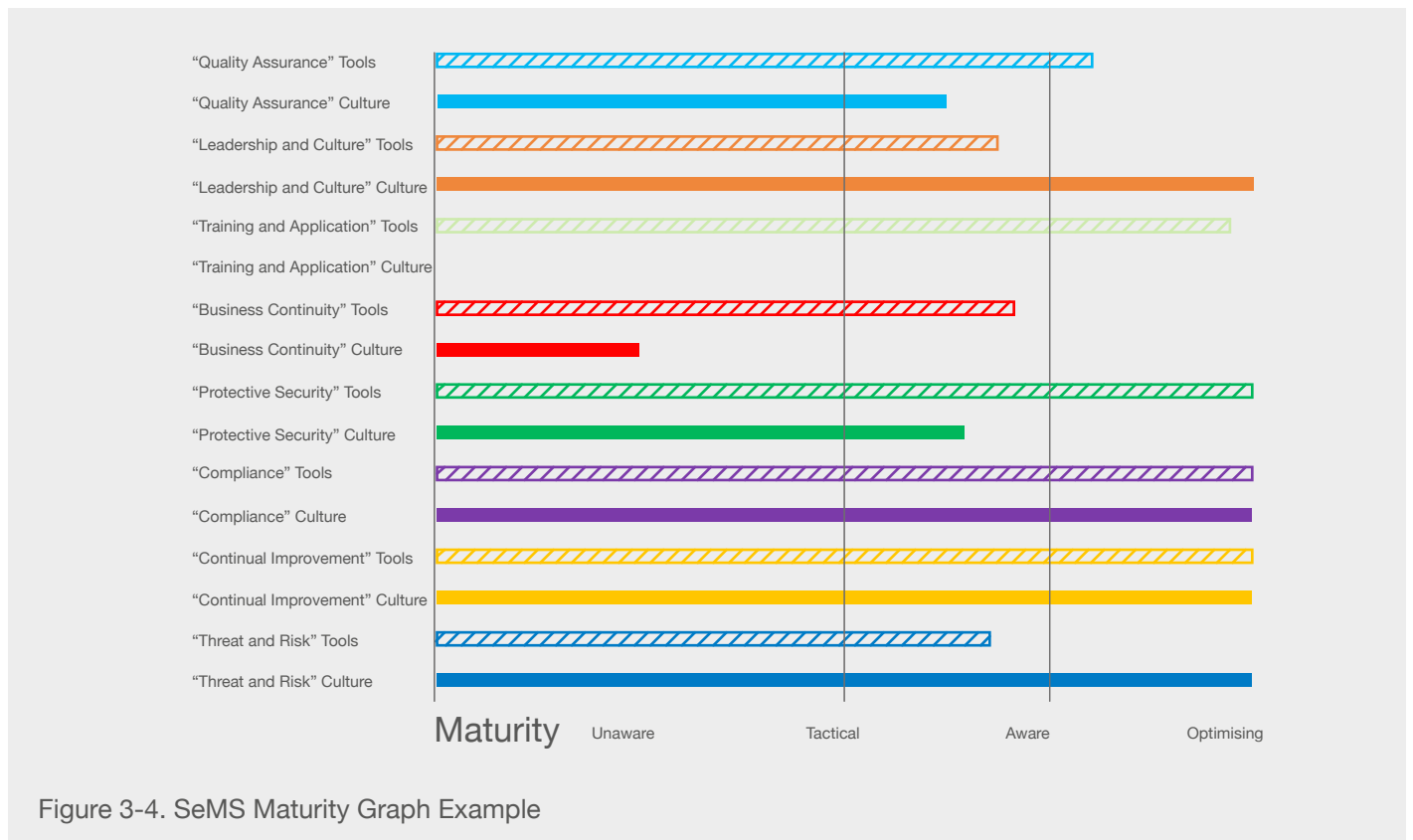


Figure 3-4. SeMS Maturity Graph Example

## Interpreting your SMAT results

---

This graph enables you to understand the relative strengths in the SeMS at your airport, as well as where improvement is required. Remember, the graph outputs are dependent upon the honesty of the answers being given, and that those answers reflect the state today, not the desired state. Also remember, there will always be a degree of subjectivity to the results, so this is not a replacement for a full process audit or deep culture assessment.

Each bar in the graph is showing maturity for that particular labeled Element. On the Results tab within the SMAT, you will see a descriptor for the maturity level of each Element. Read the descriptor for the maturity level of each Element that you have scored.

Capture each Element's maturity level in SMATs Result Worksheet. A template can be found in Appendix H.

### A special note on sub-cultures

Appendix I provides an in-depth case study outlining what you may encounter across different groups within the airport community. The case study provides suggestions on how to best think about and adapt your approach to groups whose SeMS readiness and maturity may not be in alignment. Although not uncommon, an SeMS along with SMAT Results Worksheet can be used to increase awareness of the sub-cultures and enable maturity growth over time.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Interpreting your SMAT results

### Making decisions to improve based on your SMAT result

You now need to make a number of decisions.

Like completing the SMAT, it is recommended that decisions are made on a consultative basis, and this includes Executive-level personnel. The reason the latter is recommended is because SeMS has the potential to significantly influence the security of your airport. As the people ultimately accountable for security, Executives should be included in such a decision. Furthermore, they are likely to have an influence on the effectiveness of change through demonstrable leadership (see the Leadership and Empowerment Element) and resourcing of the change.

An SMAT Results Worksheet has been provided in Appendix H to record the outcomes of this particular exercise.

#### Step 1 Determine the Ideal maturity for each Element

Refer pg. 69 for Maturity Definitions.

Record the Ideal (to be) maturity for each Element Tool and Mindset in the SMAT Results Worksheet.

#### Step 2 Identify which Element needs maturing

Using the SMAT Results Worksheet, compare the columns Current Maturity and Ideal Maturity and decide and record which Element's Tool and Mindset you wish to mature (i.e., which requires change).

#### Step 3 Prioritize Elements that need to improve

Guidance on things to consider when prioritizing efforts to mature Element Tools and/or Mindset can be found below and in more detail in Appendix E.

#### Step 4 Identify who needs to be involved in the discussions to develop the Implementation/Action Plan

Record this on the SMAT Results Worksheet.

#### Step 5 Develop an Implementation/Action Plan

Refer to guidance on pg. 74.

An Implementation/Action Plan template can be found in Appendix H.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Interpreting your SMAT results

An SeMS Result Worksheet template can be found in Appendix H. The following is a worked example:

Element		Current Maturity (From SMAT results)	Ideal Maturity Step 1	Change Required? Y/N Step 2	Priority Step 3	Who should be involved in the Implementation/Action Plan development? Step 4
Threat and Risk	Tools	<i>Optimizing</i>	<i>Optimizing</i>	No	–	–
	Mindset	<i>Aware</i>	<i>Aware</i>	No	–	–
Compliance	Tools	<i>Unaware</i>	<i>Optimizing</i>	Yes	1	<i>Enterprise Risk Management Team, Airport Security Manager, Head of Internal Quality Control, Head of IT, Learning and Development</i>
	Mindset	<i>Tactical</i>	<i>Aware</i>	Yes	–	–
Protective Security	Tools	<i>Optimizing</i>	<i>Optimizing</i>	No	–	–
	Mindset	<i>Tactical</i>	<i>Aware</i>	Yes	8	<i>Chief Financial Officer, Procurement Lead, Airport Security Manager, Chief Operating Officer</i>
Business Continuity	Tools	<i>Aware</i>	<i>Aware</i>	No	–	–
	Mindset	<i>Unaware</i>	<i>Aware</i>	Yes	4	<i>Business Continuity Manager, CFO, Training and Development</i>
Training and Application	Tools	<i>Aware</i>	<i>Aware</i>	No	–	<i>Training and Development, Procurement Lead, HR, Communications, Chief Financial Officer</i>
	Mindset	<i>Tactical</i>	<i>Aware</i>	Yes	2	<i>Training and Development, Procurement Lead, HR, Communications, Chief Financial Officer</i>



# Interpreting your SMAT results

An SeMS Result Worksheet template can be found in Appendix H. The following is a worked example:

Element		Current Maturity (From SMAT results)	Ideal Maturity Step 1	Change Required? Y/N Step 2	Priority Step 3	Who should be involved in the Implementation/Action Plan development? Step 4
Continual Improvement	Tools	<i>Tactical</i>	<i>Optimizing</i>	Yes	3	<i>Business Continuity Manager, Enterprise Risk Management Team, Chief Operating Officer, Airport Security Manager, Procurement Team Lead</i>
	Mindset	<i>Aware</i>	<i>Optimizing</i>	Yes	5	<i>Business Continuity Manager, Enterprise Risk Management Team, Chief Operating Officer, Airport Security Manager, Procurement Team Lead</i>
Just Culture and Leadership	Tools	<i>Aware</i>	<i>Optimizing</i>	Yes	7	<i>Entire Board, Communications, HR, SeMS Facilitator, SeMS Champion</i>
	Mindset	<i>Optimizing</i>	<i>Optimizing</i>	No	–	
SeMS Quality Assurance and Governance	N/A	<i>Unaware</i>	<i>Aware</i>	Yes	6	<i>SeMS Facilitator, SeMS Champion, Enterprise Risk Management, Airport Security Manager, Chief Operating Officer</i>



# Interpreting your SMAT results

## Prioritizing action to improve maturity

While it would be good to make all changes necessary to bring all Elements to the ideal maturity as soon as possible, it is recognized that this is unlikely to be feasible due to resource limitations and the time it will take to realize the changes. It is therefore appropriate to prioritize efforts to make changes. Appendix E provides detailed guidance on things to consider when prioritizing the efforts.

Record the outcome of your prioritization decisions on the SMAT Results Worksheet. The next step is to develop an action plan to progress the priorities. Now is the time to start thinking about who should be involved in that action plan. Detailed guidance on the action plan follows.

## Completing an Implementation/Action Plan to improve SeMS

Now you know the 'as is' and 'to be' or Ideal maturity level for each Element tool and mindset and have prioritized them, you are ready to start taking action towards moving from 'as is' to 'ideal'. Appendix F provides detailed guidance on actions you should consider implementing. The actions will depend on:

- Element
- Tool or mindset
- Current maturity level

For example, if your top two priorities are maturing (a) Compliance Tools, which has a current maturity level of Unaware and (b) Training and Application Mindset, which has a current maturity level of Tactical, you will:

Step 1: Refer to Appendix F.

Step 2a: Within Appendix F, go to the Compliance section > go to the Tools page > go to the Unaware to Tactical row, and choose from the list actions you consider appropriate and feasible to adopt.

Compliance		
Tools		
<b>UNAWARE to TACTICAL</b>	<ul style="list-style-type: none"><li>• Design, develop and implement an internal quality control program, including a quality control system which comprises checklists and guidance for internal inspectors and an information management system for findings results, communications, follow up action, and evidence collections.</li><li>• Ensure internal inspectors are appropriately skilled.</li><li>• Utilize the official regulatory audits findings to inform the internal quality control program.</li></ul>	

## Interpreting your SMAT results

Step 2b: Within Appendix F, go to the Training and Application section > go to the Tools page > go to the Tactical to Aware row, and choose from the list actions you consider appropriate and feasible to adopt.

### Training and Application

#### Mindset



#### TACTICAL to AWARE

- Ensure that Training Needs Analysis considers behavioral requirements to apply knowledge and skills in practice (competency based rather than knowledge based), and the wider factors that may encourage or hinder demonstration of required behavior (e.g., supervisor role modeling, work design, and cognitive load of work).
- Ensure that the Training Plan, where appropriate, includes behavioral training and practice for application, ideally in simulations.
- Ensure that any skills, knowledge, and behaviors that are trained for are considered in staff performance assessments, and included in their role profiles.

Step 3: In addition to referring to the guidance that is specific to the Element Tool or Mindset, you should also:

- a) Consider your readiness level (see Section 2.1. pg.40) as your Implementation Plan may focus on different activities.
- b) Refer to the guidance on Dependencies on Other SeMS Elements provided for each Element in Appendix F.

### Training and Application

#### Dependencies on other SeMS Elements



- Refer to Training and Application for training program development.
- It may not be appropriate that punitive action is taken for noncompliance where Leadership and Empowerment mindset maturity is low (refer to Leadership and Empowerment).
- Subject to the findings from the root cause analysis, other Elements may be relevant (e.g., Leadership and Empowerment, Training and Application, and Threat and Risk).
- An SeMS is fundamentally about risk management, but Compliance alone will not achieve this. It should therefore become a component of Continual Improvement.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Interpreting your SMAT results

---

The dependencies guidance is Element-specific but is not maturity-, tool-, or mindset-specific. Rather, it highlights where change to one Element is most likely to influence or be influenced by other Elements. This should be considered when determining what actions to include in your Implementation/Action Plan.

Step 4: Once you have determined which actions are appropriate and feasible, taking into account your readiness level and influence from or on other Elements, you can record the actions within the SMAT on the SeMS Implementation/Action Plan. A template can be found in Appendix H.

You may have other record-keeping/planning mechanisms that you prefer to use. The most important thing is that you use something that makes sense to you and that you will use to track completion of actions. Subject to the amount of change required, a program or project management approach may be appropriate in the short to medium (1–5 year) term.

### Implementing the Action Plan

You now have an action plan to implement (or further mature) your SeMS. As part of its development, like all good project management processes, the following should be identified and agreed upon:

- Resources required
- Timeframe for action
- Stakeholders
- Risks to the project/action plan
- Quality control (refer to quality assurance)
- Measures of success (consider periodic use of the SMAT)

How long it will take to implement your SeMS will depend on a number of factors, including:

- Your SeMS readiness
- Current maturity levels
- Ideal maturity levels
- Commitment by senior leadership, including the SeMS Champion
- Size and complexity of your airport
- Existing micro-cultures (e.g., the influence of the airline's organizational culture at a hub)

Using the SMAT on a periodic basis will help you determine your progress. You should, however, be mindful that depending on current and desired maturity, and if you are maturing a tool or culture, this could vary from months to years. It may take only one month to develop a quality control (Compliance Tool) but changing a hostile Compliance mindset to one that is positive could take years. Generally, maturation of tools will be faster than maturation of mindsets.

It would not be unreasonable for it to take 5–6 years before your SeMS becomes 'just the way we do security.' It is important to manage these expectations, resource accordingly, and factor this into the SeMS quality assurance process.





# Interpreting your SMAT results

---

## Conclusion

This Guidance document has been developed to assist you with establishing and maturing your airport's SeMS. It is designed so that you can use it regardless of the maturity of your SeMS – you will use a little or a lot depending on how SeMS-ready your airport is and how mature the tools and mindset of each of the seven Elements are, namely:

- 1 Threat and Risk
- 2 Compliance
- 3 Protective Security
- 4 Business Continuity, including Incident Management
- 5 Training and Application
- 6 Continual Improvement
- 7 Leadership and Empowerment

Additionally, the SMAT is designed to be used on a periodic basis in order to inform your progress as you implement the actions you have taken from the Guidance document.

The Guidance has been developed in close consultation with the US aviation market in order to capture the user's needs and preferences in terms of content and format.





# Abbreviations, Acronyms, Initialisms, and Definitions of Terms

---

BCS	Business Continuity System
BIA	Business Impact Assessment
CPTED	Crime Prevention through Environmental Design
CFO	Chief Financial Officer
DHA	Defense Health Agency
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
PARAS	Program for Applied Research in Airport Security
QMS	Quality Management System
SeMS	Security Management System
SMS	Safety Management System
TSA	Transportation Security Administration
VBIED	Vehicle Borne Improvised Explosive Device

**Audit:** An in-depth compliance examination of all aspects of the implementation of the airport security program.

**Business Continuity Management System:** Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity

**Exercise:** A full-scale security exercise is a simulated act of unlawful interference that has the objective of ensuring the adequacy of the contingency plan to cope with different types of emergencies. A partial security exercise is a simulated act of unlawful interference that has the objective of ensuring the adequacy of the responses to individual participating agencies and components of the contingency plan, such as the communications system.

**Follow-up corrective action:** Action undertaken to ensure the corrective action is compliant and effective in rectifying the deficiency(ies) identified by the quality control activity(ies).

**Inspection:** An examination of the implementation of the relevant Airport Security Program requirements by the aircraft operator, airport, or other entity involved in security.

**Protective Security:** Protective security is the measures put in place to mitigate security risks (terrorism and criminality) and meet security compliance requirements. It includes the planning, design, implementation, and operation of those measures. For the purpose of an SeMS, protective security relates to those measures that are designed for the purpose of security (e.g., CCTV and fencing), versus those measures that provide a security outcome but whose purpose is not primarily security (e.g., speed bumps).



# Abbreviations, Acronyms, Initialisms, and Definitions of Terms

---

## **Quality control activities:**

Any one of the following activities:

- Audit
- Exercise
- Follow-up corrective actions
- Inspection
- Survey
- Test

## **Quality control system:**

Policy, processes, and tools that are utilized to conduct quality control activities.

The system usually comprises:

- Authority to conduct quality control activities
- Risk-based schedule of activities
- Test protocol
- Findings database
- Inspector tool kit (e.g., checklists and prompts)
- Escalation mechanism (e.g., administration orders and enforcement action)

**Survey:** An evaluation of security needs, including the identification of vulnerabilities that could be exploited to carry out an act of unlawful interference, and the recommended corrective actions.

**Test:** A covert or overt trial of an aviation security measure that simulates an attempt to commit an unlawful event.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements

Each of the seven SeMS Elements was introduced in Section 1 of the Guidance, SeMS at a Glance. Appendix A provides additional information about those SeMS Elements. This additional information is supplementary and is provided to deepen your understanding of that particular Element.

As identified in Section 1 What SeMS is not, there will be a range of documents that inform your airport's security and should be part of your SeMS. References to those documents is included for each of the Elements in this Appendix. As this is guidance only, the references are not exhaustive, as you may have documentation that is specific to your airport.

The references are indicated by this symbol:



1

Getting to know SeMS

2

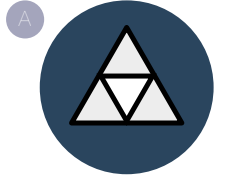
Are you SeMS ready?

3

How to establish your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Threat and Risk

A threat is an individual with the intent and capability to undertake an act of unlawful interference. Unlike other types of risks (e.g., safety), the threat in the security context is one that is intelligent in that individuals will actively:

- Avoid risk mitigation measures (e.g., bypass security measures such as screening)
- Seek out and exploit vulnerabilities (e.g., attack unprotected areas such as landside)

Risk is the manifestation of an act of unlawful interference measured by the likelihood of the event occurring (taking into account vulnerabilities) combined with the consequences if the event occurred.

SeMS is ultimately about reducing the security risks for an airport. This can be achieved by a good understanding of the threat and risk, which is achieved through credible threat information informing a robust risk assessment process and agreed position on risk appetite, followed by management of the risk (in accordance with risk appetite).

The Threat and Risk Element requires the following sets of information and input to adequately and effectively assess the potential threats and risks:

- National threat information input
- Industry risk context information
- Local risk context information, which includes analysis of quality control findings
- Consultation with stakeholders (whole section on inputs for risk assessment)
- Understanding that it is not about compliance
- Organizational agreement on:
  1. Threat scenarios
  2. Definition of likelihood
  3. Definition of consequences
  4. Calibration of risk matrix
  5. Consequences and the calibration across different consequences

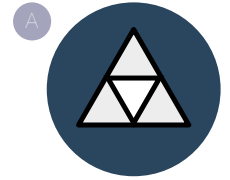
The security risk assessment model may be one that is based on other risk assessment models utilized by the airport. What must be captured in a security-specific risk assessment is the contribution of vulnerabilities to the risk, noting these will be sought out and exploited by criminals and terrorists. The risk assessment is therefore based on the following, widely referenced, risk formula:

Risk = Likelihood factor x Vulnerability factor x Consequence factor.

Managing the risk is therefore a factor of managing the likelihood, vulnerabilities, and consequences.

$$\text{Risk} = \begin{matrix} \text{Occurrence Factor} \\ \times \\ \text{Vulnerability Factor} \\ \times \\ \text{Consequence Factor} \end{matrix}$$





# More detail about the seven SeMS Elements

## Threat and Risk

---

### The Likelihood Factor

The Likelihood Factor seeks to measure the probability or possibility of an attack (or use of the airport to facilitate an attack) occurring. The measurement considers the threat (intent and capability) and the attractiveness of the target. The threat will be determined at a national level and adjusted to take account of the local environment that may cause a deviation from the national threat.

#### Example

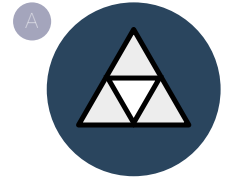
The threat is known to have the capability and willingness to use automatic weapons in an attack. Automatic weapons are relatively easy to procure given the law in this airport's state. Therefore, relative to other regions with stricter regulations, the occurrence factor will increase for an airport in this region.

### The attractiveness

The attractiveness of a target is about the appeal of the target to the perpetrators, relative other airports; effectively, how good the return on investment is for the terrorists. Consideration should be given to:

- Ease of attack—this is taken into account by the Vulnerability Factor
- How well an attack on this airport (relative to others) meets the attackers' objectives, examples of which could include the following:
  - Opportunities that could cause mass casualties—the larger the number of casualties, the greater the impact of the message being delivered.
  - Adverse economic impact—The airport makes a major economic contribution to the area, and a disruption would have a negative economic impact.
  - Symbolism—depending on the symbolic objective of the attack, an airport's location, association with certain targets (e.g., the nationality of passengers) may make it more attractive.
  - Public anxiety—public and community fear or stress is generated on a wider scale and often promulgated by media coverage.
  - High media imagery—this is often closely linked with symbolism.





# More detail about the seven SeMS Elements

## Threat and Risk

### The Vulnerability Factor

This factor is determined by how easily it would be to facilitate an attack.

Vulnerability is determined by an assessment of the infrastructure design, operations, and security culture. Infrastructure design can make an attack easier to facilitate and/or increase the attractiveness of a target.

#### Example

A drop-off point that is close to a potential target increases the ease of delivering a vehicle-borne improvised explosive device.

#### Example

The Istanbul Airport attackers were dropped off at the airport by a taxi. They requested the taxi stop in the third (furthest from terminal) traffic lane. They did this because they had conducted reconnaissance and knew that Police were only approaching vehicles that were dropping off in the first two lanes (the airport was operating at a high threat level and this Police approach to vehicles was an additional security measure).

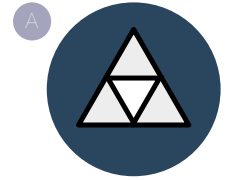
Through a live CCTV stream, a CCTV operator saw them being dropped off and became suspicious of them for various reasons. The CCTV operator contacted security personnel who followed and approached the attackers.

While the identification of suspicious activity and subsequent intervention did not prevent the attack, it may have reduced the severity of the attack.

It is known that terrorists undertake reconnaissance prior to an attack in order to determine the feasibility of their plans. It is during this time that the airport community may observe them doing this (through identification of suspicious activity) and can intervene, in turn preventing the attack entirely. A strong security culture will facilitate this intervention.







## More detail about the seven SeMS Elements

### Threat and Risk

#### The Consequence Factor

This factor is determined by the impact on the airport of an attack.

The types of consequences will depend on the threat that is being considered and what the airport considers to be important to protect. The typical types of impacts that are measured for the purpose of determining the consequence factor are:

- Fatalities and casualties, typically measured by number of people
- Business interruption, typically measured in monetary terms, but may also be measured in qualitative terms, e.g., days closed and % of flight delays—this should be considered in the context of Business Continuity
- Financial loss, obviously measured in monetary terms and should include cost of recovery and opportunity cost (during disruption)
- Reputation, sometimes measured in order of magnitude using qualitative measures such as Major (adverse mainstream media reporting) or Minor (no media reporting)—sometimes it is quantified in monetary terms using a dollar value for the qualitative measures and direct implications, e.g., share value loss

Using the above factors, with either qualitative or quantitative measures, the risk score is determined. This may be presented as a number, descriptor (e.g., High) or, as is often used, a color (Black, Red, Amber, or Green).

Those risks that exceed agreed risk appetite should be actively managed by reducing the likelihood, vulnerability, consequence, or all three.

It is appropriate, in fact necessary, that robust risk assessment processes and policies are in place. Consideration, however, should be given to how the outcomes of the risk assessment are communicated, in particular the language used. Remember that integration of security management into the business fabric is an objective of SeMS. It is therefore appropriate and likely to be more effective if the risk story is communicated in language that is appropriate for the audience.

Consider how you might interpret the following outcome of the risk assessment to these stakeholders:

- Chief Financial Officer
- Enterprise Risk Manager
- Business Continuity Manager
- HR Manager

**“Even the security people don’t use the Risk nomenclature. They use words like ‘repeated problems’, ‘we just know’, ‘trends in deficiencies’, ‘that’s what worries everyone’ not; Vulnerability, Risk Assessment, Threat.”**

2017, summary of themes from interviews with staff from large and small airports



1

Getting to know  
SeMS

2

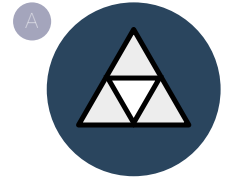
Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Threat and Risk

*“...30% of the risk items on the airport security risk register exceed our risk tolerance level of 6. To reduce those risks below risk level 6, the airport security team needs a budget increase of \$1 million this year...”*

Translating that message into language that aligns to those individuals’ interests is likely to achieve a much better outcome; for example, when speaking with the Chief Financial Officer (CFO), you may think about their role and objectives and come prepared accordingly. It is likely they will want a better understanding of where that \$1 million is to be spent, why it has to be spent that way, and what the return on investment will be. You therefore may explore and shape the discussion around the following:

- Are infrastructure projects planned that could incorporate security-by-design principles and design out security vulnerabilities in order to reduce the cost of overlaying protective security (refer to Protective Security)?
- Could operational security within existing resources be used instead of investment in high capital expenditure security systems (refer to Training and Application and Protective Security)?
- Could you demonstrate that a higher investment (capital expenditure) in one technology will provide cost savings in the long term through reduced operating expenditure? This might include security-related operating expenditure such as overtime wages and non-security related operating expenditure such as the cost of power (refer to Continual Improvement).
- Consider working through the risk assessment process with the CFO so they understand why the risk ratings are what they are. The CFO may identify some innovative solutions by better understanding the likelihood, vulnerabilities, and consequences (refer to Continual Improvement, Business Continuity, Threat and Risk, and Leadership and Empowerment).

While focused on metrics for the quality assurance of your SeMS, Appendix D will provide additional guidance on this communication issue.

Other documentation or references that you might utilize when establishing or maturing this Element are:



- *Your airport’s Airport Security Program*
- *TSA’s Public Area Security National Framework*
- *TSA’s SSI Best Practice Guide for Non-DHS Employees and Contractors*
- *CAO Aviation Security – Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*
- *DHS’s If You See Something, Say Something campaign*
- *PARAS0004 – Recommended Security Guidelines for Airport Planning, Design, and Construction*
- *DHA Public Area Security National Framework*



# More detail about the seven SeMS Elements

## Compliance



Other documentation or references that you might utilize when establishing or maturing this Element are:

- TSA Airport Security Program and 49 CFR 1542 Implementation Guidance
- 49 CFR 1542



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Protective Security

Reducing security risks can be achieved by utilizing non-security designated resources and security-designated resources.

### Example

Using public realm design to create stand-off distance—a security outcome is achieved by using non-security designated resources.

The focus of this Element is security-designated risk reduction measures, which include environmental design, physical security measures, and operational security measures.

The protective security measures to be adopted by an airport could be determined by:

- Which measures are most appropriate for reducing the risks (determined by Threat and Risk)? This might include the conduct of a cost benefit analysis.
- Compliance requirements—this is equipment that is prescribed by regulations.

## Environmental Design

Security outcomes through environmental design are achieved by the following:

- Designing out features that increase the likelihood (attractiveness of target and vulnerabilities);
- Reducing the consequences of an attack

The appeal of environmental design is that it does not require further capital or operating expenditure to maintain its security effectiveness, and can reduce the need for security measures.

The following example illustrates this concept:

### Example

The establishment of a forecourt with landscaping that incorporates hostile vehicle mitigation measures (e.g., bund), provides the stand-off distance that manages the risk through first reducing the consequence of a vehicle-borne improvised explosive device (VBIED) and secondly, reduced the attractiveness of the terminal as a VBIED-attack target. The standoff distance is established; it does not require ongoing maintenance or operations to maintain its risk-reduction ability. Furthermore, the forecourt can be incorporated into the public realm design, further strengthening the business case of the security outcome.



# More detail about the seven SeMS Elements

## Protective Security

The use of environmental design to accommodate security measures can improve the effectiveness of security measures, and in some cases reduce the amount and/or cost of those measures. The following example illustrates this concept:

### Example

The ceiling fixtures and architectural design of the terminal takes into account the need for lighting and CCTV for security purposes. The fixtures avoid the need for retrofitting fixtures and provides integrated Information and Communication Technology. The architectural design reduces the number of lighting and camera fixtures as the CCTV can work more effectively without coverage interference.

### Crime Prevention through Environmental Design (CPTED)

CPTED is the use of design and space management principles in order to manipulate human behavior. It is a crime-prevention strategy based on proper planning, design, and structure of cities, neighborhoods, precincts, or individual sites to create the effective use of the built environment, which can lead to a reduction in the fear and incidence of crime, as well as an improvement in quality of life.

The design of a particular space has to ensure that the intended activity can function properly, as well as directly support the control of behavior, in order to reduce the opportunity for crime.

Physical security is the traditional application of applying security. It is using equipment, infrastructure, and technology to manage the security risks. These include but are not limited to:

- Barriers – these can range from dynamic and static, and manual to electronically operated
- Video Surveillance
- Screening – cargo, items, goods, supplies, passengers, staff, baggage
- Intrusion Detection Systems
- Access Control Systems



Figure A-1. Example of CPTED: a wall designed to prevent graffiti





## More detail about the seven SeMS Elements

### Protective Security

The performance requirements for the individual measures should take into account:

- The reason for the application of a security measure
- The environment in which it is to operate
- How the measures will interact with the operating environment
- The necessary supporting infrastructure
- Whole-life costs including maintenance and consumables
- Maintenance requirements
- Staff skill and training needs
- Interface with existing systems



Figure A-2. CCTV Camera

Other documentation or references that you might utilize when establishing or maturing this Element are:

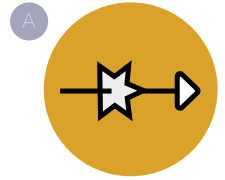


- *Your airport's Airport Security Program*
- *TSA Design Guidance such as the Planning Guidelines and Design Standards for Checked Baggage Inspection Systems (PGDS)*
- *PARAS 0004 Recommended Security Guidelines for Airport Planning, Design and Construction*
- *TSA's Public Area Security National Framework*
- *TSA's Security Guidelines for General Aviation Airport Operators and Users*
- *IATA's Airport Development Reference Manual*
- *DHS's Active Shooter Preparedness Program*
- *DHS's National Terrorism Advisory System*
- *Airport Council International's The ACI Guide to Airport Security: Assessment of Human Factors in Checkpoint Security*
- *Airport Council International's Landside Security Handbook (publication expected in 2018)*
- *TSA's Comprehensive Risk Assessment of Perimeter and Access Control Security*
- *TSA Air Cargo Screening Technology List (ACSTL)*
- *FAA AC150/5360-13A Airport Terminal Planning and Design*
- *RTCA Standards for Airport Security Access Control Systems*



# More detail about the seven SeMS Elements

## Business Continuity, including Incident Management



Other documentation or references that you might utilize when establishing or maturing this Element are:

- *Your airport's Business Continuity Program and Plans*
- *Your airport's Airport Security Program*
- *Your airport's Airport Emergency Program*
- *TSA's Intermodal Security Training and Exercise Program, also known as I-STEP*
- *TSA's Public Area Security National Framework*
- *DHS's Active Shooter Preparedness Program*





# More detail about the seven SeMS Elements

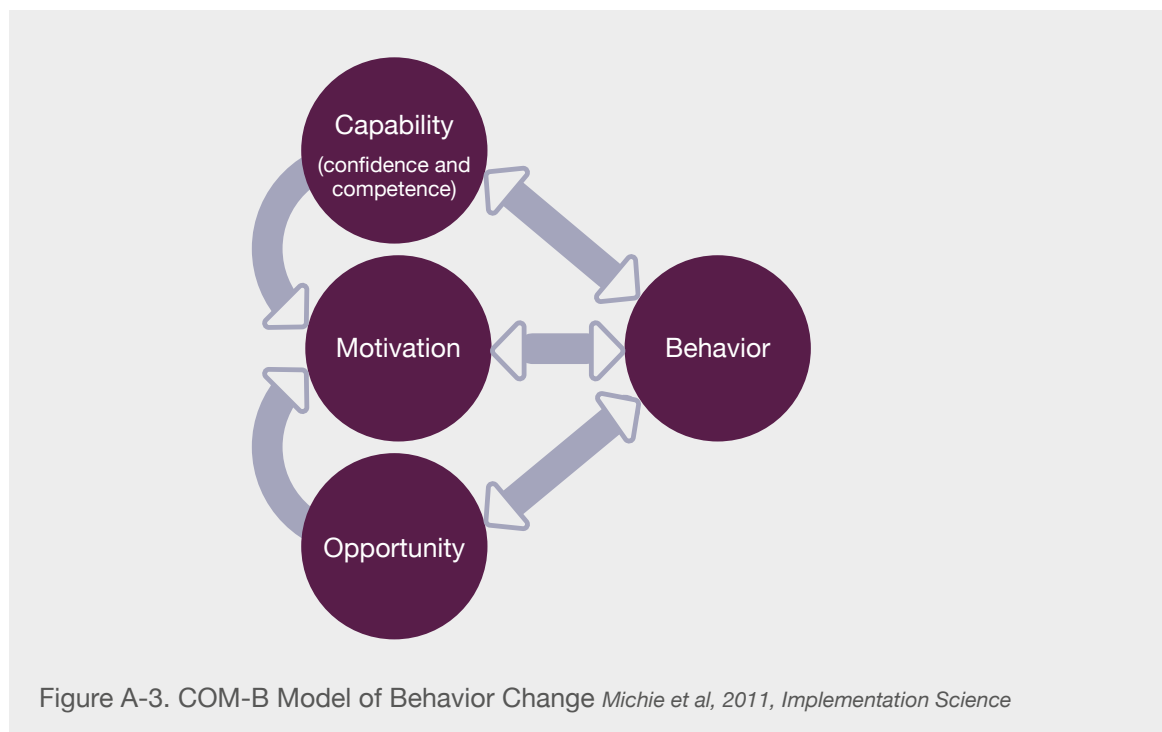
## Training and Application

People at all levels of the organization need to be equipped with sufficient and appropriate knowledge, skills, and confidence in a range of situations so that they can contribute to maintaining a secure and healthy workplace. An SeMS requires that a wide range of people, representing the wider airport community, receive training and education on both the SeMS and the role they can play, even informally, in contributing to enhanced security for the airport.

Training refers to activities undertaken to:

- Raise levels of the airport community’s security management knowledge and skills
- Provide the opportunity for the airport community members to develop confidence, ability, and desire to apply the knowledge and skills they have learned in real-life situations

The effectiveness of security-related training should be regularly evaluated, focusing in particular on whether the lessons learned are being applied effectively. Application of training refers to the requirement that security knowledge and skills are actually acted upon, and put into practice, in order for the training to be considered effective. In large part, realizing application depends on training that has been designed and delivered to act as a key enabler of behavior change, within a wider security-culture change program.







# More detail about the seven SeMS Elements

## Training and Application

Training is driven by security needs, which may be broadly split into two categories:

Discretionary training, driven by the airport's assessment of needs outside the scope of mandatory training

### Example

This might include the decision to train baristas in a vendor location on how to identify appropriately suspicious behaviors. In this case, the decision to train would have been driven by the airport's own assessment that a key opportunity for quick and early threat detection lies in the ability of those on the floor to spot and report those threats.

A training program, which may be the required airport security training program or integrated into a culture-change program, should be established to ensure a planned, regular, effective, and measurable approach is taken to build security competence and awareness. A responsible person should be designated to take ownership of ensuring training-plan development and rollout, while a business sponsor should take responsibility for championing the importance of training participation. Information on the appropriateness and effectiveness of the operator's SeMS may be gathered through some of the following:

- Informal feedback
- Risk identification reports
- Root cause analysis of quality control findings
- Discussion of security management activities in regular and planned security meetings
- Systems such as CCTV footage





# More detail about the seven SeMS Elements

## Training and Application

### Legal responsibilities

This should cover specific security obligations under the applicable legislation.

### Moral and ethical drivers for security

This will be a reflection of company values and should recognize that different ethnic and social backgrounds can yield different views on morals and ethics.

### Security threat and risk identification, risk assessment, and control tools appropriate to their role

These can range in complexity from simple observation methods (e.g., situational awareness training) to detailed quantitative methods (e.g., formal tools for business threat and risk assessment).

### Job-specific security requirements (emphasis is on job-specific)

This training should make staff aware of the known security risks and tasks in their area or line of work.

### Behavioral programs

This entails training techniques that foster behavior change beyond knowledge-sharing and awareness-building. In order to keep peoples' interest and motivation to engage in training, you may wish to update and adapt your training approaches on a regular basis.

### Workplace observation and situational awareness skills

This focus should be on the individual's own working environment and how they can change their personal security behavior.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements


## Training and Application

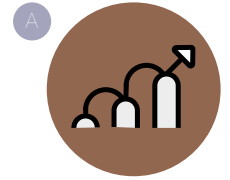
Training can take many forms including formal classroom training, simulations, meetings, on the job training, and other communication methods. In order to assess the training needs and to successfully design, develop, and implement effective and targeted training to all staff, a specific and effective process should be taken that consists of the steps listed below.

- 1 Training-needs analysis approach**
- 2 Design and development of materials, including training strategy and plan**
- 3 Delivery of training**
- 4 Evaluation of training**
- 5 Management of training**

Other documentation or references that you might utilize when establishing or maturing this Element are:

- Your airport’s Airport Security Training Program
- TSA’s Public Area Security National Framework
- DHS’s Active Shooter Preparedness Program
- DHS’s If You See Something, Say Something campaign





## More detail about the seven SeMS Elements

### Continual Improvement

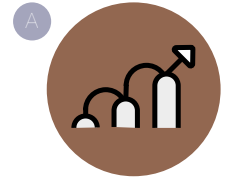
---

Security threats are evolving rapidly. With that, security risks continually change. In response, SeMS needs to constantly be one step ahead; what was effective yesterday may no longer be effective today. Continual improvement is the process of continuously assessing, and then acting to improve upon:

- Whether you are doing the things you have chosen to do, right
- Whether the things you have chosen to do were the right things to do in the first place
- Whether the assumptions you had in place to decide that those were the right things are in fact right
- The root cause of failings

To be effective in enabling improved security outcomes, Continual Improvement processes and activities need be carried out under an overarching mindset, or learning approach, that encourages behaviors required for a learning environment. In order to have an effective change in mindset, an open and fair culture is required.





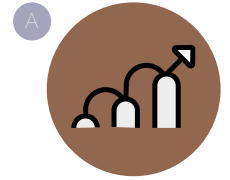
# More detail about the seven SeMS Elements

## Continual Improvement

For example, people are encouraged to develop and apply their own skills and knowledge to enhance organizational security. Staff members are updated on security issues by management, and security reports are fed back to staff so that everyone can learn the pertinent security lessons. Learning progresses from individual managers and staff to the organization, which in turn feeds into an informed and fair culture.

The mechanisms that make Continual Improvement truly effective and a fully fledged element that facilitates an increased security-aware culture could be explored in the following ways:

- Constantly looking forward and proactively assessing situations—includes risk reduction, considered decisions on risk and cost/benefit considerations.
- Reviewing and asking difficult questions about what really needs to change—how could we innovate and improve more on what we currently do?
- Build upon an existing functional organization—recognize that security must exist within a functional organization and overarch as an inherent factor across all functions and levels. Security cannot be perceived as an element in which organizations merely apply changes to functions and processes.
- Integrated security enhancing mechanisms—proactive and constant exploration of how security mechanisms can be integrated into airport operations rather than being imposed as new processes or systems.
- Risk identification should be based on a combination of threat and vulnerability information.
- Organizations should develop and maintain formal processes to identify the causes of sub-standard SeMS performance, determine the implications of sub-standard performance in operations, and seek out proactive ways to eliminate or mitigate such causes.
- Conduct a pre-mortem technique used in management as an alternative way to assist decision making. The technique utilizes predictive hindsight in which an event is imagined to have already occurred where the outcome was a failure or there was an error. The process assists teams to identify risks at the outset, by working backward to determine what potentially could lead to the failure of the project or organization.



# More detail about the seven SeMS Elements

## Continual Improvement

### What do we look at to assess this?

This Element requires an open and honest assessment of the circumstances and organizational context. A few core assessment questions that assist in identifying the level of maturity of this element include, but are not limited to, the following:

- What security-learning processes are in place?
- Are we taking proactive steps to learn from previous security successes and failures within our own airport, across airports, and across industries? Is that learning based on root cause analysis or traditional assumptions?
- Are we taking adequate steps to share knowledge and learning across organizations, where tried and tested solutions may already have been developed and are effectively in place?
- At what point is security invited into the conversation with staff, teams, and leaders alike?
- Is it seen as a retrofit, or as a key, equal partner in operations?
- Are there opportunities for any staff member, or stakeholder, to contribute?
  - Discussion forums
  - Agenda lines
  - Security moments
  - Cross-disciplinary sharing
  - Suggestion systems

In order for the aviation industry and airports to ask these questions effectively, a change in mindset is more often required, which may challenge current and learned ways of thinking or assessing information. A critical set of mindset changes may provide the right platform to have these open and honest conversations, resulting in different solutions.



1

Getting to know  
SeMS

2

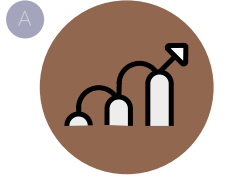
Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Continual Improvement

Some examples of where and how mindset changes can be approached or adopted leading to required changes in behavior are listed below:

- Directly ask staff where they think security improvements can be made for passengers, themselves, and the business.
- Mistakes are viewed as learning opportunities, and people are encouraged to share, without reprisal, their failures and unresolved challenges.
- Improvement discussions have periods of innovative and creative thinking.
- Discussions based on the reality and practicality of ideas are only entered into later, once options have been explored with no judgment or criticism.
- Multiple disciplines, representatives, hierarchy levels, and stakeholder roles are included in problem-solving and brainstorming discussions.
- Traditional boundaries about who is included in problem-solving are challenged, in which staff and stakeholders are included who are not traditionally thought of as partners in security questions.
- Feedback loops are included to more effectively assess not only how things have been done but also what the impact or outcome was.

### Example

You have been audited. Do you write a correction plan, and do you action it?

In deciding corrective actions, are they based on one person's opinion or are they a result of properly considered and investigated root cause activities?

### Example

You have been audited and the audit produced findings. You are considered satisfactory in all areas of the audit, and no non compliance issues are raised. Do you consider this to be job done and an indicator of the definite presence of effective security in your airport? Or do you set your own standards and ways of measuring, to determine what makes for effective security in your airport? Do you look for ways to drive your security standards and practice still higher, despite a satisfactory audit report? Do you look for ways to achieve that result again, but in a way that better aligns to other business objectives (e.g., passenger experience)?

Other documentation or references that you might utilize when establishing or maturing this Element are:

- *TSA's Security Guidelines for General Aviation Airport Operators and Users*



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Leadership and Empowerment

Culture serves as a control mechanism that guides and shapes the attitudes and behavior of staff, and as such defines the way that staff members approach security. A culture is both observed and felt, and is held in place by both formal (e.g., security policies and procedures) and informal mechanisms (e.g., lunchtime and corridor conversations and in the moment feedback).

In the security context, a positive security culture is heavily influenced by leadership from the top and within the business, and the empowerment of the airport community to do the right thing.

The effectiveness of an SeMS, and therefore a positive security culture, is greatest when first the leadership, and then all members of an organization, commit to and support security as a core value. Unfortunately, there are many examples of organizations that have SeMS processes and manuals, but their SeMS is sterilized from the start or slides into disuse due to a dysfunctional security culture. A security culture reflects the atmosphere created by everyone in the airport community that shapes the attitudes about security among the people involved in the operation. The security culture is affected by factors such as:

- Management’s actions and priorities
- Policies and procedures
- Supervisory practices
- Security planning, objectives, and goals
- Actions in response to unsafe behaviors
- Staff training and motivation
- Staff involvement or buy-in
- Staff motivation and capability to do the right thing
- Mechanisms that facilitate staff to do the right thing
- Mechanisms that demonstrate that doing the right thing makes a difference
- An organizational culture that is fair and reasonable

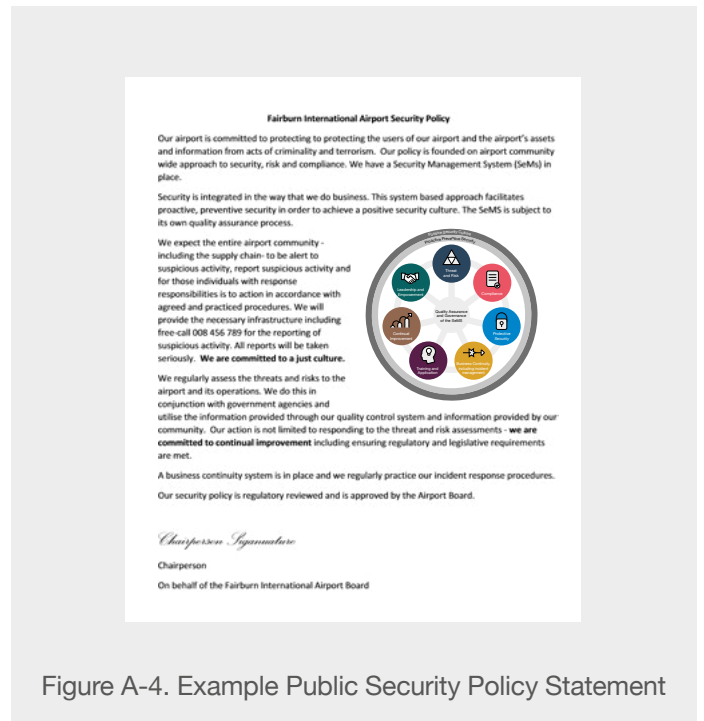


Figure A-4. Example Public Security Policy Statement



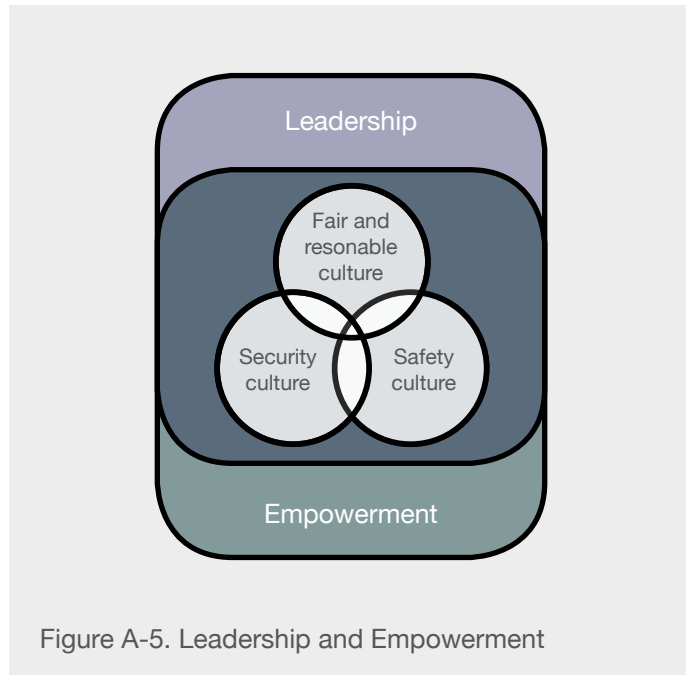




# More detail about the seven SeMS Elements

## Leadership and Empowerment

Culture is a complex concept to understand; the following illustration is an attempt to model what it means in the context of SeMS:



The security culture enables or hampers an organization’s Security Management System, and directly influences security performance. A positive security culture must be generated from the top down. It starts with the corporate Security Policy and is built on the principles and actions of management.

*International Standard for Business Aircraft Operations (IBAC) – 2012*

Figure A-5. Leadership and Empowerment



## More detail about the seven SeMS Elements

### Leadership and Empowerment

Leadership in this context is senior management consistently demonstrating commitment to security. Leadership and commitment can be determined by:

#### 1 Behavior

- Does Leadership say one thing but act in a conflicting manner?
- Does the Security Champion act in a manner that is consistent with the SeMS establishment needs?
- Is there an SeMS Champion and do their Leadership colleagues support them in their SeMS related efforts?
- Is security viewed as a value-add to the airport? Or is security viewed as a compliance risk and cost center only?
- Do they foster a climate in which there is a positive attitude towards criticisms, comments, and feedback from lower levels of the organization on security matters? Or is there a sense that leadership's view is the only view that matters, and they use their influence to force their views on subordinates?
- Do they encourage root cause analysis or is blame placed on individuals or teams when there is a failing?
- Do they proactively support preventive security or is there a view that it will never happen to us?

Culture can be dysfunctional if the shared values of the staff are not aligned with the values and objectives of the organization. If the workplace culture does not encourage, support and value security, no SeMS can succeed in improving. As each new security procedure or initiative is introduced, the reigning culture will determine new ways to avoid complying and continue doing things “the way we do things round here”.

Queensland Mining Industry Health and Security Conference Proceedings – 1999



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



## More detail about the seven SeMS Elements

### Leadership and Empowerment

#### 2 The priority given to security

- Is security a regular agenda item on meetings and does it get addressed? Or is that agenda item dispensable when time is short?
- Is there a demonstrable understanding of security risk at the leadership level?
- Is there a public security policy? Is it regularly reviewed? Where does it fit in the policy hierarchy?
- Is security talked about as a valuable element of business? How is it portrayed in public documentation such as the Annual Report?
- Is security an element of the airport's vision and values?
- Is security a core element of the enterprise risk management framework?

Empowerment is when the airport community has the desire, motivation, and mechanisms to do the right thing when it comes to security. Doing the right thing goes beyond being compliant with security rules, but includes community members being proactive in their security behavior. This is shown in community members being alert to security risks, vulnerabilities, others' behavior, suspicious activity, and mistakes, and then doing something about it in order to have the issue resolved, even if they are not involved in the resolution. It is effectively about knowing what to do when they just know something is not right no matter how vague 'something not right' may be.

Being alert comes from having a sense of community, wanting to protect the airport and its community, responding to gut feelings, and the knowledge of what to be alert to. The first item comes from the general climate of the airport. The knowledge of what to be alert to is a combination of listening to their own gut-feel and instinct as well as information learned through education.

Taking action following the identification of something that is not right is a combination of the individual's own motivation and the mechanisms that facilitate action. The motivation again comes from the climate whereas the mechanisms are systems and processes provided by the airport that, importantly, are known about and readily available. Many airports have the mechanisms but the community does not know they are available, so while someone might want to take action, they do not know how.

**In order for the SeMS to work it is essential to have a positive security culture. Creation of an informed, learning, reporting, and just culture is not a simple task but is an extremely important success factor.**

International Business Aviation Council (IBAC), 2012



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# More detail about the seven SeMS Elements

## Leadership and Empowerment

The general climate might be referred to as a fair and reasonable organizational culture (when it is right for the establishment and operation of an SeMS). It is characterized by behavior in leadership and people that encourages and supports alertness and action to be taken. To achieve this, it is important that the staff know and agree on what is acceptable and what is unacceptable security behavior. While it is recognized that slips, lapses, mistakes, and violations may occur, and the associated circumstances need to be addressed, it is understood that gross negligence or serious offenses are not, and cannot, be tolerated. A culture that is representative of this is often referred to as being firm and fair.

Mechanisms are the systems that enable the person to implement their action and include such things as 1-800 hotline numbers and online reporting systems.

For the mechanisms to be effective, they must be readily available. This could include use of easy to remember and free-call telephone numbers; campaigns promoting the use of the systems; cell phone apps to the reporting system; phone number documented on day-to-day items (e.g., lanyards), posters in staff rooms, and on telephone handsets, and listed as priority contact in employer-issued cell phones; and regular SeMS updates/reminders.

It is important that the community see that the action they take is making a difference, and this might even extend to rewarding action that is the right thing to do, such as reporting suspicious activity. This could be achieved by conducting tests such as leaving unattended items, observing the community's action, and rewarding the individuals who identify and report. When considering how to provide evidence that their action is making a difference and/or rewarding the right behavior, thought needs to be given to:

- How information is validated or followed up if the reporting system is confidential
- Sensitivity of the action taken (e.g., legal action), in response to reporting
- Reward system discouraging false reporting or contrived action

**“Training gets you to awareness level, culture piece takes it to implementation level”**

**“Culture development doesn’t have to equate to money”**

2017, Interviewees, large and small airport employees

Other documentation or references that you might utilize when establishing or maturing this Element are:

- Your airport’s public policy statement
- Your airport’s Annual Report
- Your airport’s and others’ experiences with Safety Management Systems (SMS)
- DHS’s See Something, Say Something campaign



# SMS and SeMS – similarities and differences



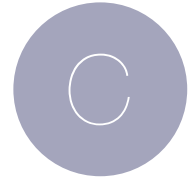
System characteristic	Safety Management System (SMS)	Security Management System (SeMS)	SMS and SeMS Comparison
Involvement of the entire airport community	<p>All about safety decision making throughout the organization</p> <p>Responsibility for safety includes those who do not have safety-designated responsibilities (e.g., baggage handler).</p>	<p>All about security decision making throughout the organization</p> <p>Responsibility for security includes those who do not have security-designated responsibilities (e.g., barista).</p>	Similar/Same
Resourcing	As the system is to be integrated, it is not intended that a separate division or department be established for SMS management or operation. That said, champions within existing operational department aid in SMS development and implementation.	As the system is to be integrated, it is not intended that a separate division or department be established for SeMS management or operation. That said, as SeMS is being established, the Guidance recommends that an SeMS Champion in the Executive staff and an SeMS Facilitator is identified.	Similar/Same although SeMS Guidance recommends identification of an SeMS Champion and SeMS Facilitator during the SeMS establishment period.
Integrated with business	It is not separate or distinct from operations.	It is not separate or distinct from operations.	Similar/Same
The system is regulated	ICAO requires states to ensure the establishment of an SMS.	<p>There is no regulatory requirement to have an SeMS.</p> <p>ICAO does not require states to ensure the establishment of an SeMS, although the benefits are increasingly being discussed in ICAO forums.</p>	Different
Scope		SeMS can be adopted by any aviation organization. This Guidance is focused on airports (of any size and complexity of operations).	Different



# SMS and SeMS – similarities and differences

System characteristic	Safety Management System (SMS)	Security Management System (SeMS)	SMS and SeMS Comparison
Continuous Improvement	Using reporting data, continuous improvement initiatives and methods are developed and implemented.	Continuous improvement is a specific Element of SeMS.	Similar/Same
Influence on culture	<p>An SMS includes requirements that will enhance the safety attitudes of an organization by changing the safety culture of leadership, management, and employees.</p> <p>Creating a safety culture sits within the SMS component Safety Promotion, and senior management’s commitment sits within the SMS component Safety Policy.</p> <p>Safety culture is an outcome of SMS.</p>	<p>The intent of an SeMS is to establish and maintain a positive security culture. An SeMS recognizes that good security is made up of tools and mindset. SeMS-related efforts focus on both tools and mindset.</p> <p>An SeMS recognizes that senior management’s commitment is required alongside an organizational culture that is fair and reasonable, and encourages personnel to do the right thing. An SeMS has captured this within the Element Leadership and Empowerment.</p> <p>Security culture is an outcome from SeMS.</p>	<p>Similar/Same in terms of the intent of changing culture.</p> <p>Different in that SeMS differentiates between tools and mindset when developing and maintaining SeMS elements.</p> <p>Different in how the contribution is recognized in each concept—the contribution of organizational culture and senior management is captured in:</p> <p>Separate components for SMS, namely ‘Promotion’ and ‘Policy,’ respectively</p> <p>One element for SeMS, namely Leadership and Empowerment</p>
Systems approach	Systems-focused like a quality management system	Systems-focused like a quality management system	Similar/Same
Components/ Elements	<p>Composed of four functional components:</p> <ul style="list-style-type: none"> <li>• Policy</li> <li>• Risk Management</li> <li>• Assurance</li> <li>• Promotion</li> </ul>	<p>Composed of Governance and Quality Assurance of the SeMS itself plus seven Elements:</p> <ul style="list-style-type: none"> <li>• Threat and Risk</li> <li>• Compliance</li> <li>• Protective Security</li> <li>• Business Continuity</li> <li>• Training and Application</li> <li>• Continual Improvement</li> <li>• Leadership and Empowerment</li> </ul>	<p>Different, although the intent of the SMS Components are similar to the SeMS Elements (e.g., the intent of Leadership and Empowerment [SeMS] is reflected in Safety Policy [SMS]).</p> <p>An SeMS’s Quality Assurance is about quality assurance of the SeMS itself, whereas the Assurance component of SMS is about assurance of safety in the business (i.e., an SMS outcome).</p>





The barista at a café in the check-in area notices a suitcase has been left unattended next to one of the check-in desks. Using the Toll-Free Number for 'See, Hear, Report' he phones through the details. The 800# is operated by the Airport Operations Center (AOC).



- Threat and Risk: There is a risk associated with an unattended bag.
- Protective Security: The 'See, Hear, Report' program, including the system and infrastructure to support its operation, is in place.
- Training and application: The barista is aware of suspicious activity, knows what to do about it, and takes action on that knowledge.
- Empowerment: Not only does the barista know what to do when he identifies suspicious activity, he feels empowered and safe to do that action. Despite it taking time away from his job, he knows that he will not be penalized for doing so. Furthermore, he knows that his call will be taken seriously and acted upon.

His call is answered and he is advised that a Security Guard will be deployed immediately. The decision to deploy immediately is made because the AOC officer answering the phone knows the current threat level is High and that the conduct of reconnaissance and testing of security measures (including response) is a method adopted by terrorists.



- Threat and Risk: Despite not being security personnel, the AOC personnel know what the current threat level is and take this into account in their decision making.
- Protective Security: The See, Hear, Report program, including the system and infrastructure to support its operation, is in place. The communication between the AOC and security team are in place and operate effectively.
- Training and application: The AOC personnel have the knowledge and skills to make an assessment of how to respond.
- Empowerment: The barista knows that his phone call will be answered and his report will be taken seriously.





# Case study

Utilizing their Hidden Obvious Typical (HOT) principle training, the Security Guard determines the unattended luggage as suspicious. She contacts the AOC to advise of her assessment.



- **Threat and Risk:** The current threat level is high and staff are aware of that. This is taken into account by the Security Guard when she applies the HOT principles.
- **Protective Security:** Security Guards are a security measure.
- **Business Continuity:** The incident response procedures are developed and available to the personnel involved in the incident.
- **Training and application:** The Security Guard has the skills and knowledge to assess a suspicious item. Furthermore, she knows what to do with that assessment. The AOC will commence the incident-response process.
- **Empowerment:** The Security Guard and AOC respect each other’s role and assessments and will take action accordingly.

The Emergency Response procedures are activated, which include:

- Security Guards deploying to the Muster Points to inspect the area for suspicious items. It is decided that one of the Muster Points is not to be used as there is an unknown vehicle parked next to it. This is communicated to the Evacuation Leaders through the Airport’s Business Continuity App loaded on all the Duty Manager phones.
- The check-in personnel and the duty managers from each of the retail outlets assist in setting up a cordon around the suspicious item. The retail staff and other personnel facilitate the orderly evacuation of the people in the terminal. They know which Muster Point is not to be used.



- **Threat and Risk:** The current threat level is high and staff are aware of that.
- **Protective Security:** Security guards are a security measure. The policy and procedures for emergency response are pre-determined, clear, and communicated to those with a need to know.
- **Business Continuity:** The emergency response procedures are developed and available to the personnel involved in the incident. The communication mechanisms across teams are in place and work effectively. The emergency response procedures have been exercised.
- **Training and application:** All personnel are aware of their own role in the emergency response process and they take action accordingly. The hierarchy of decision making is pre-determined and well known by all. The training and application is not limited to security personnel.
- **Continual improvement:** The emergency response procedures are activated quickly, efficiently, and at a relatively low level of stress because most of the personnel have been involved in an exercise program.
- **Empowerment:** All personnel involved feel empowered to take action in accordance with their training. The hierarchy of decision making is pre-determined, well known, and respected by all.





# Case study

The Police respond and determine the item is safe. The Evacuation Leaders activate the Recovery Plan that they have received through the Incident Response App.



- Threat and Risk: The current threat level is high and staff are aware of that.
- Protective Security: The Police are an integrated security resource. All relevant personnel have access to a phone with the relevant App already loaded and tested.
- Business Continuity: The Police are an integrated resource in the emergency response arrangements. The Recovery Plan is predetermined, well known and exercised. The App provides for a consistent message; therefore, there is a coordinated response and reduced risk associated with erroneous and inconsistent messages and rumors.
- Training and application: All personnel are aware of their own role in the Recovery process, and they take action accordingly. The hierarchy of decision making is predetermined and well known by all. The training and application is not limited to security personnel.
- Continual improvement: The Recovery Plan has been tested and exercised so people can take action with confidence and efficiency
- Empowerment: All personnel involved feel empowered to take action in accordance with their training.

Using the Business Continuity App, the staff provides feedback. A review of the incident is conducted. Lessons learned are identified and issued to parties for action.



- Threat and Risk: The current threat level is high and staff are aware of that.
- Protective Security: The Police are an integrated security resource. All relevant personnel have access to a phone with the relevant App already loaded and tested.
- Business Continuity: The Police are an integrated resource in the emergency response arrangements. The Recovery Plan is predetermined, well known, and exercised. The App provides for a consistent message; therefore, there is a coordinated response and reduced risk associated with erroneous and inconsistent messages and rumors.
- Training and application: All personnel are aware of their own role in the Recovery process, and they take action accordingly. The hierarchy of decision making is predetermined and well known by all. The training and application is not limited to security personnel.
- Continual improvement: The Recovery Plan has been tested and exercised so people can take action with confidence and efficiency.
- Empowerment: All personnel involved feel empowered to take action in accordance with their training.



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices



# Case study

A follow-up of the lessons learned is scheduled into the Internal Quality Control Annual Schedule.



- Threat and Risk: The current threat level is high and staff are aware of that.
- Compliance: Follow-up of the lessons learned from the incident are scheduled into the Internal Quality Control Annual Schedule.
- Protective Security: The lessons learned take account of the security response mechanisms including hardware (e.g., communications technology) effectiveness, efficiency, and appropriateness.
- Business Continuity: Business Continuity policies and procedures are reviewed in the context of the incident. Changes are made and communicated accordingly.
- Training and application: Personnel's knowledge and application of skills are reviewed. For identified deficiencies, root cause analysis and action are taken accordingly.
- Continual improvement: Lessons learned are identified and actioned.
- Empowerment: All personnel involved in the lessons learned are open, honest, and candid in their contribution.



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices

# Quality assurance of your SeMS



As described above, Quality Assurance is the system that determines the ongoing effectiveness of the SeMS. The quality assurance system will have policies, processes, and tools to be developed and utilized by the SeMS Facilitator to assess the system’s performance against criteria to be agreed upon by the organization. Consistent with the spirit of SeMS, it would be appropriate that quality assurance is integrated into the Airport’s quality management system rather than as a standalone system operated independently by the SeMS Facilitator or security team.

Figure D-1 illustrates the typical process for undertaking quality assurance. Behind each of those steps will be policies, processes, and tools:

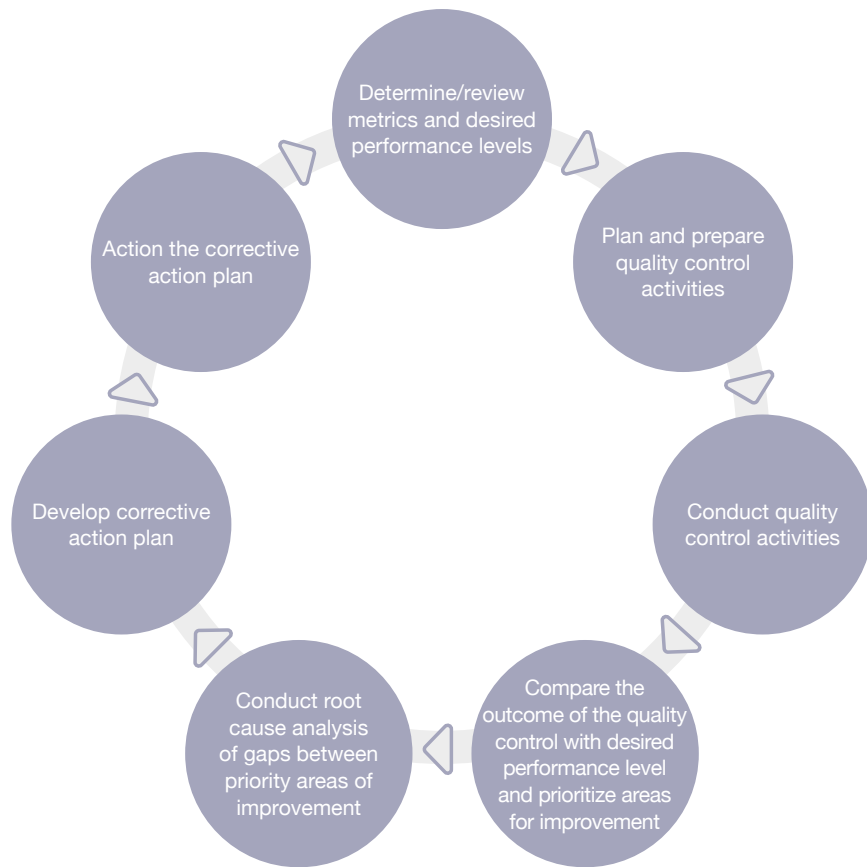


Figure D-1. Quality Assurance Steps

While the quality assurance policy, process, and tools (and corrective action) are integrated into the business, what should be unique to the SeMS are the metrics used to measure its effectiveness.

## Quality assurance of your SeMS

---

Use of appropriate metrics allows Security to speak to airport management using business language and is therefore a valuable tool in informing and influencing senior management, particularly when the security message is framed in the context and language of organizational risk and return on investment.

To be of value, however, the metrics must be credible, and therefore must be evaluated. ASIS International provides a Security Metrics Evaluation Tool (SMET) that can be used to assess the quality of chosen metrics. The SMET utilizes the following evaluation criteria:

- Reliability
- Validity
- Generalizability
- Cost
- Timeliness
- Manipulation
- Return on Investment
- Organizational relevance
- Communication

For communicating the metrics to senior management, consideration might be given to the following:

- Present metrics that are aligned to the airport's organizational objectives.
- Present metrics to measure the specific issues in which management is most interested.
- Communicate the value of the resources that are threatened and the consequences if a security event occurs (when the metric is prevention-focused).
- Communicate how there is movement towards a strategic goal.
- Present the data regularly at a frequency that is appropriate to its purpose.

When developing or improving the SeMS, it is important to give thought to how you may assure the business that it is effective and efficient. As with any system, there are a number of key questions to answer:

- Will it deliver the required results?
- How will it be maintained and kept up to date?
- How do we ensure that it will be followed?
- How do we ensure that it will be complete and fit for the purpose?

Having a clear understanding of the goals and objectives for the SeMS and the key customers, (e.g., the traveling public [in the context of safety] and the Airport Executives [in the context of retaining asset value]) is vital if effective assessment criteria are to be established to determine the SeMS success (or areas for improvement). Understanding this when designing your quality assurance process will enable you to collect the right data at the right time, and in turn, improve efficiency, reliability, and credibility of the quality assurance process and its associated metrics.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# Things to consider when prioritizing efforts to further mature Elements' tools and mindset

While it would be good to make all changes necessary to bring all Elements to the ideal maturity as soon as possible, it is recognized that this is unlikely to be feasible due to resource limitations and the time it will take to realize the changes. It is therefore appropriate to prioritize efforts to make change. The following provides a list of considerations when prioritizing:

**Threat information.** Does the threat information tell us that we should focus on one Element more than another?

**Existing mindset.** Is there a mindset within the airport community that will support particular change efforts? Should those changes therefore be prioritized because they will be easier to achieve?

**The relative return on investment.** When comparing all the changes that are required, do some investments (change per Element) realize a greater return? Investments might include:

- Staff, including quantity, levels, cost, and opportunity cost
- Funding
- Leadership input

**How quickly can the change occur?** It may be that having a number of quick wins generates buy-in for the SeMS and builds momentum and support for those change efforts that might take longer.

**We just need to get started.** It is likely that a large amount of change, e.g., moving from Unaware to Optimizing will take a lot of time to be realized. It may be more appropriate that some change is commenced as soon as possible.

**Ease of access to resources.** The time at which the SMAT-related decisions occur relative to the financial year and budget requests may be important. Obtaining funding out of the budget cycle can be difficult. Can change reliant upon funding be postponed until a more effective time in the budget cycle? Or can the change efforts be funded within existing budget resources?

**Strategic funding.** The ability to secure strategic funding (over a number of financial years) may be helpful, so that short term and smaller budget changes can occur.

**Other priorities.** Are there other business priorities or initiatives that require the same resources? Are there other business priorities or initiatives that would complement the SeMS change management efforts? Are there other business priorities or initiatives that might conflict with SeMS change management efforts?

**What is the amount of other change that is going on in the business?** Too much change can undermine efforts as organizations experience change fatigue. It may be more effective to focus on one large change program than multiple small efforts.

**What is Leadership interested in?** As we have seen from the Leadership and Empowerment Element, leadership buy-in and demonstrable commitment to security is essential to SeMS success. It may be that particular Elements interest (for various reasons) the Leadership. Engaging them through that interest will assist with solidifying ongoing support for an SeMS.



## What actions can I take to improve the maturity of the SeMS Elements?

---

The following provides guidance on the actions you may wish to take to move an Element's tool or mindset from one maturity level to another (e.g., moving Leadership and Empowerment Tool from Aware to Optimizing). It also provides guidance on how an Element may influence or be influenced by other Elements.

How to use this action guidance:

- 1 Once you know each Element's Tool and Mindset 'as is' and 'to be' maturity levels and priorities, go first to the relevant Element's section within this Appendix. Use the color code to navigate (e.g., [Leadership and Empowerment green](#)).
- 2 Once you are in that section, turn to that Element's Tool or Mindset page (e.g., Tool).
- 3 Go to the row that describes the maturing action that you are seeking (e.g., Aware to Optimizing).
- 4 Read the list of action items the guidance recommends and choose those that you consider appropriate and feasible for your airport.
- 5 You should also refer to the Dependencies on other SeMS Elements guidance in each Element's section. This section will provide information on how that Element will be influenced by or influence other Elements (e.g., it may not be appropriate that punitive action is taken for non-compliance where Empowerment and Leadership maturity is low. Refer also to Compliance.)



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



# Threat and Risk

## Mindset

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Ensure that prior to threat and risk assessments being put into action, there is a clear communication campaign and training behind the why and how these assessments can be used to enable better security outcomes.</li> <li>• Identify specific questions, such as, “How might we better identify and report Suspicious Activity?” to start conversations and workshops in the airport. Use these conversations and workshops to raise awareness and gather information to inform the design of full campaigns, which can later be rolled out to the airport.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Actively promote the wide participation of different airport community groups in threat and risk assessment activities (e.g., data gathering).</li> <li>• Use information gathered from the conversations you have held (see Unaware to Tactical, above) to identify barriers and enablers that discourage and encourage reporting.</li> <li>• Design specific campaigns, (e.g., Reporting Suspicious Activity) that take account of the barriers and enablers identified.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Ensure that wide participation of different airport community groups in the threat and risk identification system becomes business as usual.</li> <li>• Ensure that specific campaigns, such as Reporting Suspicious Activity, have other actions associated with them in order to activate enablers to reporting (e.g., supervisor role modeling) and to remove barriers to reporting (e.g., parallel stream that trains those receiving suspicious activity reports to take reports seriously and to act professionally and with encouragement when receiving reports).</li> <li>• Celebrate and communicate the successes arising from the community’s awareness and reporting. Consideration must be given to the sharing of sensitive information and/or discouraging false reporting, particularly if the celebration system includes a reward component.</li> <li>• Ensure threat and risk are included as a natural part of Executive/Board level decision-making, integrated within business as usual decision-making.</li> <li>• Ensure you consider the effect of behaviors on use of specific tools to identify threat and risk. For example, if providing a dedicated security reporting line, you should provide training for those receiving calls (including tone and manner when receiving submissions); ensure data collected is analyzed, and any trends and actions cascaded to appropriate risk and action registers; and ensure actions are closed out and any successes publicized (in broad terms, exact details of changes made are not required).</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Continual Improvement Section.</li> <li>• Threat and risk briefings are a standing agenda item on Executive/Board meetings.</li> <li>• Security and Finance together utilize the risk assessment to determine the budget allocation for security risk reduction measures.</li> </ul>





# Threat and Risk

## Tools

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Develop and implement a suspicious activity awareness raising campaign (refer to Threat and Risk Mindset guidance material, for more description of how you may want to go about this). Refer to Appendix G for a template to developing a simple communications strategy.</li> <li>• Establish regular contact with the local intelligence and police agencies.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Establish a (confidential) reporting system (e.g., suspicious activity) and other reporting.</li> <li>• Obtain regular threat information/briefings from the intelligence and police agencies.</li> <li>• Review and update the risk assessment matrix in accordance with the threat information.</li> <li>• Agree on the airport’s risk appetite policy in the context of the risk assessment matrix (e.g., risk reduction measures will be identified for all risk events of score 6 and above).</li> <li>• Implement the risk reduction measures identified by the risk matrix.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Commence briefings to the Executives on the current threat and risk assessment outcomes.</li> <li>• Ensure the threat and risk briefings are a standing agenda item on the Executive and Board meetings.</li> <li>• Celebrate and communicate the successes arising from the community’s awareness and reporting. Consideration must be given to the sharing of sensitive information and/or discouraging false reporting, particularly if the celebration system includes a reward component.</li> <li>• Establish and implement arrangements with the government agency community for the airport to provide intelligence (in the form of raw data) to the relevant government agencies (e.g., the information provided through the confidential reporting system).</li> <li>• Undertake analysis of the information in the confidential reporting system to identify trends in vulnerabilities and/or threats.</li> <li>• Commence analysis of government agency threat information and local threat information.</li> <li>• Ensure the critical functions identified by the Business Impact Assessment (BIA) conducted for the Business Continuity System (BCS) are incorporated into the security risk assessment process.</li> <li>• Develop and utilize a cost benefit analysis tool to support the risk appetite policy.</li> <li>• Set up governance arrangements so that Security and Finance together utilize the risk assessment to determine the budget allocation for security risk reduction measures.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Continual Improvement and Business Continuity Elements.</li> <li>• Ensure the threat and risk briefings are a standing agenda item on the Executive and Board meetings.</li> <li>• Set up governance arrangements so that Security and Finance together utilize the risk assessment to determine the budget allocation for security risk reduction measures.</li> </ul>







## Threat and Risk

### Dependencies on other SeMS Elements

- While security focused, the SeMS campaign may be led by the Airport's Communications Team with technical support from the Security Team.
- Fair and reasonable or just-culture requirements for anonymous reporting (e.g., no blame attitude) should be established and training required of those receiving calls.
- A risk-based approach to determining security measures will align to Continual Improvement, so efforts driven by these respective Elements should be aligned.
- Refer to Business Continuity for the identification of critical assets and the security risks that may cause disruption.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Compliance

## Mindset



<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• When implementing your quality control program, use the first iteration of it as a dry run to act as an awareness raising, learning, and discussion exercise. Outputs in this dry run are seen as learning experiences, and feedback from participants is used to further improve the program prior to its full implementation.</li> <li>• If you already have a quality control program in place, assess its effectiveness and the degree of buy-in to the process (e.g., through feedback surveys, one-to-one interviews, observation, and focus groups) to help identify what is and is not working with it currently.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Use feedback to improve your compliance process, and to identify where you might need to better communicate the why of compliance and the benefits it brings to the airport and individuals working within it.</li> <li>• Pay attention to how user friendly your compliance process is, and to what degree it is used as an opportunity to learn how to improve rather than as a punitive exercise.</li> <li>• Ensure inspectors know how to conduct proper root cause analysis investigations, including considerations of human factor design and behavioral causes of non-compliance.</li> <li>• Consider how to train your inspectors in people skills (e.g., active listening and giving feedback), so that they can help champion the use of compliance and quality control activities in a spirit of learning rather than pure checklist exercises.</li> <li>• Actively acknowledge the activity and effort that goes into compliance activities, and praise efforts from those who positively contribute to its implementation.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Conduct regular high level reviews of your compliance process (e.g., every 2 years), to ensure their effectiveness and user-friendliness.</li> <li>• Regularly consider whether advancements in technology might make the internal quality control process more efficient and people friendly to carry out.</li> <li>• Invite regulatory audit bodies to your airport to engage with your airport staff affected by their audits, hear their experiences of the audit process, and answer questions regarding the regulatory audit (the why and how the information is used).</li> <li>• Consider engaging with regulatory audit bodies, to identify improvements and enhancements that could make the external audit process more effective and user friendly.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Continual Improvement Section.</li> <li>• Celebrate and communicate compliance improvements.</li> </ul>



## Compliance

### Tools



<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Design, develop, and implement an internal quality control program including a quality control system comprising checklists and guidance for internal inspectors and an information management system for findings results, communications, follow-up action, and evidence collections.</li> <li>• Ensure internal inspectors are appropriately skilled.</li> <li>• Utilize the official regulatory audit findings to inform the internal quality control program.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Integrate the official regulatory audit findings with internal quality control findings.</li> <li>• Analyze quality control findings in order to identify root causes of non-compliance.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Focus on using Continual Improvement to facilitate compliance.</li> <li>• Cross reference findings from the confidential reporting system and compliance findings to identify any relationships and/or indications of root causes of deficiencies.</li> <li>• Put in arrangements so that Leadership allocates resources to rectify non-compliances (as a demonstration of commitment to improvement rather than punitive action).</li> <li>• As part of the Compliance findings analysis, identify compliance improvements so that they can be communicated and celebrated.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Continual Improvement.</li> <li>• Communicate and celebrate compliance improvements.</li> </ul>

## Compliance

### Dependencies on other SeMS Elements



<ul style="list-style-type: none"> <li>• Refer to Training and Application for training program development.</li> <li>• It may not be appropriate that punitive action is taken for non-compliance where Leadership and Empowerment maturity is low. Refer to Leadership and Empowerment.</li> <li>• Subject to the findings from the root cause analysis, other Elements may be relevant (e.g., Leadership and Empowerment, Training and Application, and Threat and Risk).</li> <li>• An SeMS is fundamentally about risk management, but Compliance alone will not achieve this. It should therefore become a component of Continual Improvement.</li> </ul>
---



# Protective Security

## Mindset



<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Ensure the reason for carrying out compliance requirements and risk assessments (see Threat and Risk) is communicated to those involved in the process.</li> <li>• As far as possible, communicate with those whose area of work is affected by factors assessed in compliance checks/risk assessments. Use this as an opportunity to help them understand how their actions contribute to risk management and mitigation, and how that benefits the airport as a whole.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Have conversations, workshops, and agenda items with a wide range of airport operations functions and stakeholders to discuss how attending to protective security is everyone's business.</li> <li>• Engage widely with other operations, functions, and stakeholders within the airport (e.g., commercial, maintenance, tenants, and marketing) to understand their perspectives on protective security. Use these perspectives to identify ways to meet their needs in an integrated manner (e.g., ways to enhance security screening process that demonstrate care for customer as well as a smooth check-in process).</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Gather and share examples of protective security contributing to good business, with clear long-term benefits realizable for the bottom line, passenger/customer experience, and airport community quality of work experience.</li> <li>• Ensure line managers recognize and reward individual contributions, however small, to enhanced compliance through instant verbal recognition and praise.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to the Continual Improvement Section.</li> <li>• Incorporate considerations of security into value considerations for other business objectives such as passenger experience, asset management, and organization reputation.</li> </ul>



# Protective Security

## Tools



<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Use compliance requirements and risk assessments (see Threat and Risk) to determine protective security needs.</li> <li>• Establish an equipment/system maintenance regime.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Continue to use compliance requirements and risk assessments (see Threat and Risk) to determine protective security needs.</li> <li>• Continue to implement the equipment/system maintenance regime.</li> <li>• Integrate the procurement regime into the Airport’s broader procurement program.</li> <li>• Ensure that protective security arrangements take into account operational and physical security, and that the relationship between them is considered holistically (e.g., a CCTV system is not effective if there are no arrangements in place for personnel to respond to what the CCTV sees).</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Consider other design and operational disciplines when seeking a security outcome (e.g., public realm design is used to manage the hostile vehicle risk).</li> <li>• Measure the whole of life cost of physical security measures when considering different security solutions.</li> <li>• Establish a proactive (versus reactive) maintenance program.</li> <li>• Take into account other design and operational disciplines to facilitate efficient use of security needs (e.g., lighting, architecture, and security work together to design lighting and infrastructure to minimize the number of CCTV cameras needed without compromising the security outcome).</li> <li>• Assess the impact on passenger experience and ensure that other business considerations are taken into account for security efficiency.</li> <li>• Quantify in monetary terms the value of risk reduction measures in order to determine the return on investment. Communicating the return on investment to project and finance managers may assist with future support requests.</li> <li>• Volunteer the airport to partake in live trials.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to the Continual Improvement Section.</li> <li>• Incorporate the value of security into the value of other business objectives such as passenger experience, asset management, and organization reputation.</li> <li>• Consider how security outcomes can be achieved through design disciplines, and operational and physical security.</li> </ul>



# Protective Security



## Dependencies on other SeMS Elements

- Some protective security requirements will be driven by regulatory requirements; therefore, refer also to Compliance.
- Protective security requirements should be determined by their contribution to reducing security risks; therefore, refer also to Threat and Risk.
- The effectiveness of physical security equipment/systems is often reliant on the operators; therefore, refer also to Training and Application.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Business Continuity



## Mindset

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Run a short incident scenario exercise with parties who are required to contribute to, manage, use, or drive use of the Airport Emergency Plan. Use the outputs of this scenario to discuss the importance of the Airport Emergency Plan in enabling the airport to continue to work effectively.</li> <li>• Clearly describe the processes required, at minimum, to develop and adhere to incident response procedures.</li> <li>• Ensure clear requirements are in place for contribution to, engagement with, and awareness training of the Airport Emergency Plan and incident response procedures.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Put in place a regular schedule of simulations and scenarios (see Tools, below). Ensure these are run in an atmosphere of learning, and highlight the role that practice has in developing habits of behavior.</li> <li>• Ensure feedback and learning exercises take into account the effects of stress and unfamiliar situations on human behavior, and that this is fully considered and discussed.</li> <li>• Use the simulations and scenarios to test the practices currently in place. Be prepared to question whether current processes and systems are fit for their purposes.</li> <li>• Consider using a regular series of short simulations and scenarios/walk-throughs rather than few one-off big exercises. Behavior change requires practice, short and often (even 10 minutes at the end of a meeting once a month is more effective than only once a year).</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• When debriefing exercises, focus on competencies and behaviors (e.g., information gathering, situational awareness, adaptability, working under stress, and ambiguity) rather than adherence only to linear procedure.</li> <li>• Enhance training by including elements that coach staff on how to help others in times of stress and pressure, as well as becoming aware of and managing their own internal stress reactions (e.g., training on power and authority dynamics and how these affect communication during times of stress/acute danger).</li> <li>• Focus on differentiating between what individuals can control and what they cannot during incidents. Emphasize this in training and practice. Ensure that factors that were unique and uncontrollable in a situation do not overshadow discussion on those factors that can be controlled.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Continual Improvement.</li> <li>• Obtain and maintain ISO 22301 Certification.</li> </ul>



## Business Continuity



### Tools

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Ensure the Airport Emergency Plan is compliant, and all involved parties are familiar with their roles and responsibilities and are resourced appropriately.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Develop and implement an incident response exercise program.</li> <li>• Action the exercise lessons learned.</li> <li>• Incorporate the exercise lessons learned.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Design, develop, and implement a Business Continuity System (BCS). Ideally security is part of the BCS for the entire airport. In the absence of an airport BCS, one can be developed for Security.</li> <li>• Findings from the BCS development, e.g., from the Business Impact Assessment (BIA), are captured and incorporated as part of Continuous Improvement.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Obtain and maintain ISO 22301 Certification.</li> </ul>

## Business Continuity



### Dependencies on other SeMS Elements

- Actioning the lessons learned will be linked with Continual Improvement.
- The security risk assessment will influence the prioritization of business continuity development and maintenance; therefore, refer also to Threat and Risk.







## Training and Application

### Mindset

#### UNAWARE to TACTICAL

- Ensure that any Training Needs Analysis activities are accompanied by clear messaging of why the needs analysis is taking place and how it informs the design of relevant training for the target audience.
- Ensure those conducting the Training Needs Analysis are trained and competent to do so, and are using best practice tools and techniques relevant to the particular type of training being considered (e.g., opinion surveys, skills surveys, observation, shadowing, incident analysis, performance data review, interviews, assessment, and focus groups).

#### TACTICAL to AWARE

- Ensure that Training Needs Analysis considers behavioral requirements to apply knowledge and skills in practice (competency based rather than knowledge based), and the wider factors that may encourage or hinder demonstration of required behavior (e.g., supervisor role modeling, work design, and cognitive load of work).
- Ensure that the Training Plan, where appropriate, includes behavioral training and practice for application, ideally in simulations.
- Ensure that any skills, knowledge, and behaviors that are trained for are considered in staff performance assessments and included in their role profiles.

#### AWARE to OPTIMIZING

- In the Training Plan, identify areas where training content across operational functions and other stakeholders can be integrated to avoid unnecessary silos, overlaps, or repetitions across groups.
- In the Training Plan, identify opportunities for different operational functions and stakeholders to learn together, in order to further build networks and relationships across the airport.
- In Training Design, ensure tools and techniques to encourage behavioral change are used. Effective security training focuses on providing experiences to: connect with others in the airport community; develop applied competence in areas such as situational awareness and effective response under stress conditions; and connect with how to enact the airport's vision and values through security behavior.
- Build Training Evaluation into the Training Plan, including baseline measures taken prior to training delivery, against which later measures can be compared for improvement. These measures can range from very simple (e.g., reactions to training through surveys) to sophisticated (e.g., business results such as decrease in number of incidents since training occurred).
- Ensure Evaluation occurs immediately after training completion, as well as longer term (e.g., 12 to 18 months). This is to assess whether the behavior is becoming embedded in the system.
- Ensure senior management sponsors and promotes training across the entire Organization.

#### MAINTAINING OPTIMIZING

- Refer to Continual Improvement Section.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices



## Training and Application

### Tools

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Carry out a Training Needs Analysis.</li> <li>• Create a Training Strategy and Plan.</li> <li>• Execute the Training Plan.</li> <li>• Track training against the plan and intended strategic outcomes annually.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Enhance the Airport Training Plan to include all airport community members (not only those individuals with security designated functions).</li> <li>• Design, develop, and deploy training in accordance with the enhanced training program.</li> <li>• Ensure that training includes identification and resolution of suspicious activity.</li> <li>• Conduct formal covert tests on staff with security responsibilities.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Establish and implement a training quality control program. The quality control should be about testing individuals' understanding and effectiveness of application.</li> <li>• Test not only that people know what to do when they identify suspicious activity, but they are empowered to do so.</li> <li>• Test that the skills through the entire suspicious activity identification and resolution are effective, and people are empowered to apply them.</li> <li>• Integrate the Airport Security Training Program with other training plans within the airport (e.g., performance management and customer relations).</li> <li>• Develop a system that quantifies the value of the training in order to measure the return on investment.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Ensure that results from Application testing are fed into the Continual Improvement efforts.</li> <li>• Share the return on investment with HR and Finance in order to demonstrate value, and therefore secure further support in the future.</li> </ul>

## Training and Application

### Dependencies on other SeMS Elements



- Consider how this relates to your Leadership and Empowerment maturity; for example, it may not be appropriate to apply punitive action in response to test failures where Leadership and Empowerment and Training and Application are not mature.
- Consider how this relates to Continual Improvement maturity.
- Consider how this relates to your Compliance maturity.
- The training quality control program may be linked with the internal quality control program, but must measure effectiveness of training and not just compliance (i.e., training has been conducted x times per year).
- Testing of community members' knowledge of security requirements may be linked with the Communications Strategy if it is implemented (refer to Threat and Risk).



# Continual Improvement

## Mindset



<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Use the outputs of assessments (e.g., the SMAT in this Guidance or industry standards) to hold discussions that highlight the need for regular review of whether processes and practices are working.</li> <li>• When incidents occur, ensure that they are used as an opportunity to examine whether current improvement practices are adequate.</li> <li>• Use assessments, audits, interviews, and collation of historic data to identify any trends in failure or low performance that do not seem to be addressed. Have conversations with relevant stakeholders regarding the potential impact of this continued trend.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Evaluate the use and performance of specific campaigns (e.g., Reporting Suspicious Activity Awareness Raising). Use the outputs of these evaluations to prompt discussion on ways to improve.</li> <li>• Seek to include the wider airport community in any evaluations and discussions for improvement.</li> <li>• Pay particular attention to the contributions of all stakeholders within the wider community in terms of threat and risk data and suggestions for improvement.</li> <li>• Ask specific questions on the enablers and barriers that might encourage or discourage reporting.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Ensure, to the degree that it is appropriate, feedback is regularly made available to the wider airport community in terms of threat and risk activities. Data and trends can be anonymized, for example, or reported in more general terms.</li> <li>• Ensure those involved in lessons learned discussions and reviews are familiar with tools and techniques to examine unconscious assumptions when evaluating systems, incidents, and performance.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to Leadership and Empowerment.</li> </ul>





# Continual Improvement

## Tools

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Develop, design, resource, and implement an internal quality control program that focuses on compliance and effectiveness.</li> <li>• Review formal regulatory audit and compliance outcomes.</li> <li>• Develop, resource, and implement a corrective action plan. The corrective action plan should include a cost benefit analysis and prioritization of corrective actions. This will present security as a business benefit and the use of business language will assist with discussions associated with resources.</li> <li>• Refer to Training and Application for the skill development necessary for application of quality control.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Update the internal quality control program based on quality control activities conducted to date.</li> <li>• Maintain focus of internal quality control on compliance and effectiveness.</li> <li>• Refer to Training and Application for the skill development necessary for application of quality control.</li> <li>• Invite non-security and management personnel (e.g., retail staff) to observe exercises.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Establish mechanisms that encourage operational staff to identify better ways of working (e.g., pre-mortem exercise). ‘Better’ could focus on security outcomes and other business objectives (e.g., passenger experience, efficiency, and cost savings).</li> <li>• Increase the frequency of exercises. Exercises need not be full-scale field exercises, but rather, discussion and desktop exercises.</li> <li>• Include non-security and management personnel (e.g., retail personnel) as active players in the exercises.</li> <li>• Utilize external exercise facilitators in order to draw on the benefits of independent views and others’ experience.</li> <li>• Include threat and risk as a standing item for Executive/Board level decision-making meetings.</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Reward efforts that focus on better ways of working. ‘Better’ could focus on security outcomes and other business objectives (e.g., passenger experience, efficiency, and cost savings).</li> <li>• Facilitate the involvement, as players, of non-security and management personnel in Exercises.</li> <li>• Observe other airports’ Exercises.</li> </ul>



## Continual Improvement

### Dependencies on other SeMS Elements



- Exercises are a key element of a robust Business Continuity System and subject to the airport's program and the quality control program; therefore, refer to Business Continuity and Compliance.
- Proactive engagement, including reporting, requires Leadership and Empowerment. Refer to Leadership and Empowerment.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Leadership and Empowerment



## Mindset

### UNAWARE to TACTICAL

- Ensure senior leadership comment and review of security messaging.
- Use interactive discussions, first-hand accounts, guest speakers, and case studies of security failures to increase the knowledge of the Executives and C-suite.
- Ensure any expert briefings to senior leadership include opportunity for Q&A, and open a non-judgmental discussion of the barriers senior leadership perceives in implementing enhanced security in the airport.
- Make visible within senior leadership circles the business impact of security incidents (e.g., reputation, commercial performance, and staff retention).
- Share examples of leading practice from airports of similar size and complexity.
- Identify a champion within Executives and C-Suite who can take the lead on the tone and content of security items discussed on meeting agendas.

### TACTICAL to AWARE

- Ensure that security initiatives are spearheaded by leadership and are supported (e.g., opening of events by Executives and communications issued by Executives).
- Identify any benefits of enhanced security activities against overall strategic business objectives in a series of facilitated leadership discussions.
- Identify alignment between organization values and security objectives in facilitated leadership sessions.
- Identify any barriers or myths that may inhibit good security practice in your organization (e.g., the myth that security is sufficient if there is a physical barrier in place or the myth that security is the role only of those with formal security designation).
- Identify key influencers in your stakeholder groups who may not yet be championing the security message. This includes those who may currently be influential and resistant to the changes required. Engage with these influencers directly to understand their questions and concerns, and identify where you might work together to better realize the benefits of effective security management.



# Leadership and Empowerment



## Mindset cont.

### **AWARE to OPTIMIZING**

- Identify an approach for engaging any stakeholder groups that you may not yet have engaged with— who are the voices less heard who play a part in your security ecosystem? Examples might be concessionaires, airlines, airport associated suppliers/activities, (e.g., taxi drivers and food delivery), extended security services network, (e.g., local police, local emergency response, local action groups, and local government), frequent flyers, and people dropping off and collecting passengers.
- Identify and put into practice mechanisms to engage with the groups identified above. For example, use observation, interviews, and day-in-life techniques to understand where these stakeholder groups are most likely to encounter information or be able to influence security, and use those touch points constructively. For example, ‘look and notice’ signs at drop off and pick up points, speaking engagements at stakeholder premises, and invitations to carry out joint training and simulation sessions could be helpful.
- Intentionally make use of opportunities for leadership to demonstrate links between good business, good ethics, relevant organizational values, and security behaviors. For example, this could be practiced in town hall meetings, roadshows, office walk-throughs, awareness days, and security awareness challenges.
- Use participatory methods with extended stakeholder groups to establish ‘what good looks like’ from a security perspective (e.g., interactive displays or drop-in sessions).

### **MAINTAINING OPTIMIZING**

- Refer to the Continual Improvement Section.
- Ensure that new leadership, whether through internal transition or a new hire, is inducted into the airport’s ethos of security, and links to values, business objectives, and expectations in terms of role-modeling security leadership and just culture.
- Hold leadership self-reviews, where open and honest discussion is had between leadership to self-assess and provide feedback to each other in terms of how well they feel they are exhibiting security leadership and just culture.
- Engage outside, neutral, and independent ‘eye’ to provide observation and insight regarding leadership visibility and role modeling.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Leadership and Empowerment



## Tools

<p><b>UNAWARE to TACTICAL</b></p>	<ul style="list-style-type: none"> <li>• Increase the security knowledge of Executives and C-suite.</li> <li>• Invite the local Police and intelligence agencies to brief the Executive and C-suite management on the local threat and risk context.</li> <li>• Establish a multi-agency Airport Security Committee.</li> <li>• Develop a public statement on the Airport’s security policy for communication in the airport community (communication is to be led by leadership).</li> <li>• Ensure that Security is a standing agenda item on all Board/Executive/Cross-division meetings regardless of the meeting’s objective.</li> </ul>
<p><b>TACTICAL to AWARE</b></p>	<ul style="list-style-type: none"> <li>• Conduct a just culture review through surveys, interviews, focus groups, and observation.</li> <li>• Review current performance management practices, including management of error both formally and informally, with specific focus on whether investigation and remedial activities are both fair and allocate appropriate accountability.</li> <li>• Provide training to staff on just culture ethos and its relationship to security and security management.</li> <li>• Publicize security learnings or incidents through security moments in meetings, security stand-downs, security news shots, case studies, and story sharing. Ensure Executive and C-Suite senior leadership role model these actions.</li> <li>• Identify any benefits of enhanced security activities against overall strategic business objectives in a series of facilitated leadership discussions.</li> <li>• Establish links between security activities and potential business benefits for other airport stakeholders through discussion with those stakeholders.</li> </ul>
<p><b>AWARE to OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Work with Executive support staff and the Communications team to ensure that Executives’ communications include references to the benefits of the security mindset to the business. Consider using communication opportunities that are not of a security-specific agenda.</li> <li>• Identify and act upon opportunities for broader aviation industry relationship development and engagement (e.g., other airports and aviation security forums).</li> </ul>
<p><b>MAINTAINING OPTIMIZING</b></p>	<ul style="list-style-type: none"> <li>• Refer to the Continual Improvement Section.</li> <li>• Ensure that new leadership, whether through internal transition or a new hire, is inducted into the airport’s ethos of security and links to values, business objectives, and expectations in terms of role-modeling security leadership and just culture.</li> <li>• Hold leadership self-reviews, where open and honest discussion is had between leadership to self-assess and provide feedback to each other in terms of how well they feel they are exhibiting security leadership and just culture.</li> <li>• Engage outside, neutral, and independent ‘eye’ to provide observation and insight regarding leadership visibility and role modeling.</li> </ul>





# Leadership and Empowerment



## Dependencies on other SeMS Elements

- It may not be appropriate that punitive action is taken for non-compliance where Leadership and Empowerment maturity is low. Refer to Compliance.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Template for a Communications Campaign Strategy



The following is a template to guide you on developing a communications campaign strategy.

**Strategy Objective:** What you are seeking to achieve through this communication campaign

**Example**

Example: To increase the airport community’s awareness of suspicious activity and advise them on what to do if they identify suspicious activity.

**Strategy Governance:** Identify who is responsible for the strategy’s development and implementation and how that will occur.

**Example**

The Communications Team Lead is responsible for developing and maintaining the Suspicious Activity Communications Campaign Strategy in consultation with the Airport Security Manager. The Airport Security Committee will review and approve the Strategy on an annual basis. The review will include a review of the measurement outcomes (see below). Resourcing of implementation is described below.

**Audience:** Identify who it is that you are communicating with.

**Example**

- Terminal tenants
- Airside tenants
- Landside tenants
- On-site government agencies including police
- Security personnel
- All airline ground staff and their agents’ staff
- All airport executives
- Airport operator employees – management and team leaders
- Airport operator employees – operational level
- Public transport drivers
- Taxi drivers
- Terminal cleaners
- Hotel staff
- Carpark attendants



# Template for a Communications Campaign Strategy

**Measurement:** Describe how you will measure success.

Example

One month after the communication launch and every 6 months thereafter, we will conduct a sample survey by way of a 5-minute face-to-face questionnaire with 100 staff who work at the airport. Individuals will be randomly selected but will be a representation of the above audience. The survey will be developed to measure peoples’ knowledge of suspicious activity, knowledge of what to do about it, and if they have changed their behavior in response to the training. The survey will be developed and delivered by the Communications Team in consultation with the Security Team.

**Key Message:** Use something that is simple and memorable.

Example

**See Something Say Something.** You are a key contributor to our Airport’s security. Be alert to suspicious activity. Suspicious activity is anything that causes you concern because it looks out of the ordinary. When you identify suspicious activity, immediately call free: 121212.

**Channels and Timelines:** What methods of communication will you use and when will they be utilized?

Example

- Posters in staff facilities rotated on a 2-month basis
- Suspicious Activity article in the airport’s monthly newsletter
- Lanyards to be issued with airport badges ‘See Something Say Something Ph: 121212’
- PA announcement in the terminal 2 times per hour, “You are a key contributor to our airport’s security. If you see something suspicious, please report it immediately. You can call free 121212 or approach anyone of our staff.”
- FIDS displays
- Staff SMS alert one time per month, “You are critical to our airport’s security. See Something Say Something Ph: 121212.”



# Template for a Communications Campaign Strategy

---

**Resourcing:** Identify the resources required to implement the Strategy.

## Example

- Library of five posters with 200 copies of each = \$500, one-time cost
- Lanyards = Badge office to budget for 1000 lanyards per year at a cost of 50c/lanyard
- Monthly rotation of posters = One day every 2 months for one Communication Team member
- SMS alert = No cost once arranged with the Airport Operations Center
- FIDS display = No cost once arranged with the Airport Operations Center
- Terminal PA = No cost once arranged with the Airport Operations Center



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# SeMS Readiness Results



SeMS Readiness Assessment period:

SeMS Readiness Assessment facilitated by (name and title):

*Circle the quadrant that is your SeMS Readiness result.*

Option 1: SeMS as a process	Option 2: SeMS as a system	
<p>(A1) Watching</p> <p>Descriptors of this readiness level:</p> <ul style="list-style-type: none"> <li>• An SeMS is of some interest to the airport. Interest may not yet have turned into action.</li> <li>• There may be indecision regarding how exactly to drive an SeMS.</li> <li>• There is an expectation for a clearly defined and described set of standards and documents, which explain the exact processes and content to be used to implement an SeMS.</li> </ul>	<p>(A2) Exploring</p> <p>Descriptors of this readiness level:</p> <ul style="list-style-type: none"> <li>• An SeMS might be assumed to be inherently embedded throughout their system already.</li> <li>• There may be pockets of security improvement activity in different parts of the airport that may not yet be joined up.</li> <li>• There may be ongoing conversations about how to intentionally focus on improving security in the airport, without necessarily having set up a specific project or clearly defined set of activities.</li> </ul>	<p>Option A: low urgency</p>
<p>(B1) Doing</p> <p>Descriptors of this readiness level:</p> <ul style="list-style-type: none"> <li>• Likely already are implementing SeMS standards, processes, templates, and policies, and adapting an established system such as Safety Management Systems.</li> <li>• May have an established team that is tasked with implementing an SeMS.</li> <li>• This team could be in the process of putting together, or actively seeking to find, a clearly defined set of documents that explain the exact processes and content to be used to implement an SeMS.</li> </ul>	<p>(B2) Evolving</p> <p>Descriptors of this readiness level:</p> <ul style="list-style-type: none"> <li>• Likely already are defining, together with the broader airport community what an SeMS looks like as an overarching system.</li> <li>• May have taskforces or working groups, or clearly identified individuals or teams, working to co-define an approach to security improvement across the airport.</li> <li>• There may be a number of security initiatives in place to learn and evolve from, in order to connect different parts of the airport system for enhanced security outcomes.</li> </ul>	<p>Option B: high urgency</p>



1

Getting to know SeMS

2

Are you SeMS ready?

3

How to establish your SeMS

4

Appendices

# SMAT Results Worksheet

SeMS Readiness Assessment period:

SeMS Readiness Assessment facilitated by (name and title):

*For guidance on completing this worksheet, refer to Section 1.4.*

Element		Current Maturity (From SMAT results)	Ideal Maturity Step 1	Change Required? Y/N Step 2	Priority Step 3	Who should be involved in the Implementation/Action Plan development? Step 4
Threat and Risk	Tools					
	Mindset					
Compliance	Tools					
	Mindset					
Protective Security	Tools					
	Mindset					
Business Continuity	Tools					
	Mindset					
Training and Application	Tools					
	Mindset					
Continual Improvement	Tools					
	Mindset					
Just Culture and Leadership	Tools					
	Mindset					
SeMS Quality Assurance and Governance	N/A					



# SeMS Implementation/Action Plan

SeMS Readiness Assessment Date (refer SeMS Readiness Worksheet):  
 SMAT Assessment Results Date (refer date of record from SeMS Assessments Results Worksheet):  
 SeMS Facilitator (name and title):  
 SeMS Champion (name and title):

*For guidance on completing this worksheet, refer to pgs. 75-76.*

Element	Tool or Mindset		
Current Maturity	Ideal Maturity		
Action items	By when?	By whom?	R/A/C/I?*

*\*Identify who is:  
 (R) Responsible—assigned to do the work  
 (A) Accountable—has final decision and ultimate ownership  
 (C) to be Consulted before any action or decision is taken  
 (I) to be kept Informed of what has been decided*

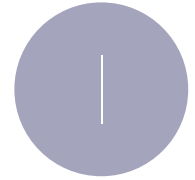
# SeMS Implementation/Action Plan

Element		Tool or Mindset		
Current Maturity		Ideal Maturity		
Action items		By when?	By whom?	R/A/C/I?*

Element		Tool or Mindset		
Current Maturity		Ideal Maturity		
Action items		By when?	By whom?	R/A/C/I?*

\*Identify who is:  
 (R) Responsible—assigned to do the work  
 (A) Accountable—has final decision and ultimate ownership  
 (C) to be Consulted before any action or decision is taken  
 (I) to be kept Informed of what has been decided





# Case study – Implementing SeMS across differing levels of readiness and maturity

The following fictional case study explores what you might encounter when diverse groups of people within the airport community are at different SeMS readiness and maturity levels. Ways to respond are then suggested.

Although this case study centers on a large airport as an example, the principles and dynamics are just as applicable to smaller airports. Any airport community will be made up of different groups of people who might not be aligned in terms of SeMS readiness and maturity levels.

## The situation

You are an SeMS Facilitator at a large international airport. Your airport has many different stakeholders who carry out activities within the wider airport footprint. Not all of these stakeholders are employed directly by your airport. For example, the airport has many tenants (retail and food) an airport hotel, and many contract staff in operations who carry out infrastructure works and improvements. A large airline also operates from a hub within the airport.

You decide to carry out SMAT exercises with different groups across the airport stakeholders. You notice, as you carry out the assessments, that there seem to be clear pockets of perception for how mature the SeMS is on different Elements, depending on the stakeholder group you are working with. You also have some one-to-one conversations and interviews with people in different stakeholder groups to start to understand what SeMS means to them and how they see it working at the airport.

With your SeMS maturity appearing inconsistent across groups, you decide that you want to start some communications and training campaigns, as well as some cross-stakeholder security working groups. This will help everyone understand what SeMS is and how they can play a part in improving security at the airport. As you start putting these activities in place, you find yourself having some interesting conversations and interactions.

## The airport hotel

You ask to conduct training with hotel staff in order to enhance their security situational awareness. Also, you want to put up some posters in staff canteen areas containing the new anonymous reporting line. The General Manager of the hotel says she is happy for you to do this and puts you in touch with the Hotel Training Manager. As the training gets underway, you find understanding is quite low. You also find that those who are attending the training are dubious of what is being suggested to them. They say, for example, that the aim of the hotel is customer satisfaction, and that the hotel motto is to ‘never say no’ to a guest. It seems unlikely that they will report suspicious behavior, even if they see something a little odd and they know the number to report it. If they have just one incident where they unnecessarily embarrass a guest, they feel it will look bad for their hotel. You realize that the training and reporting line is unlikely to result in any real behavior change in the staff who work for the hotel.

# Case study – Implementing SeMS across differing levels of readiness and maturity

## The airline

The airline is not happy for you to put up posters with your new anonymous reporting line number. The airline wants to know what is wrong with their staff using the airline's own reporting number that they have had in place for several years now and has been working really well for them. They are happy with the idea of the security situational awareness training, though, as it augments what they already have in place. Staff members are very busy, and already receive routine security training, so they want to know if they can have a shorter version of training than the version you are providing to the wider airport. The airline has its own version of SeMS in place, but it is quite different to your approach. You would like them to take on your version, but they really are not happy with this idea.

## Your own procurement and finance people

You have had a difficult time getting the kind of security training that you want approved through procurement. You want a trainer who provides security situational awareness training, which is different from simply sharing procedures on how to report an incident. You need a training provider who understands the drivers of situational awareness and the psychological reasons why people may not report suspicious behavior even when they know the right number to call. It is not easy to find the training provider that you want, but you eventually find a supplier that meets your standards. The people who sign the contracts are not happy with the supplier, saying it is too expensive, and that the training you are requesting is not appropriate for security. It takes various conversations for you to get approval, and you are not confident that the funding will be approved in the next financial year.

## What is going on here?

Airports are made up of many stakeholders, some of whom may not work directly for the airport or who belong to separate groups within the airport community. This can mean that they see themselves (naturally and possibly unconsciously) first and foremost as belonging to their primary employer, or to the group that they work within day to day. They may not naturally consider themselves to be part of the broader airport community and may not be thinking with this big picture mindset.

In this particular case, the airline hub has a very clear identity, as does the airport hotel. In fact, these identities, and their resulting mindsets and tools relating to security, are very strong and actually constitute their own micro-cultures within the wider airport community. The airline has its own mature security processes and procedures and ways of thinking about security that might not be an exact match to your approach. The hotel has a very specific set of values and expectations for what customer service looks like, and it differs with how your airport views customer service. The procurement and finance people work with each other day in and day out and may spend a lot of time thinking about things other than security. They might be very used to thinking in terms of tangible costs and benefits, and might not be used to being asked to think differently.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

# Case study – Implementing SeMS across differing levels of readiness and maturity

---

The airline might also be at the ‘Doing’ SeMS readiness level already, with some of its systems being more mature than your own. The hotel, in contrast, might be at a ‘Watching’ SeMS readiness level. At the same time, you might consider yourself and the wider airport to be at ‘Exploring’ readiness. Even within your own airport, you might find that certain groups of people or departments, in this case people related to your procurement and finance process, might not be as mature on some Elements as others.

## What might the implications of this be?

In SeMS, as described in this Guidance, the focus is on having the whole airport community acting together, consistently across stakeholder groups, to bring SeMS to life. Having a micro-culture makes it challenging to create this consistency across stakeholder groups. This in turn might lead to vulnerabilities within your security system. For example, if hotel staff members are unlikely to report suspicious behavior, an active shooter could possibly use a hotel room as an active shooter position. Delays in sharing of information between the airline’s reporting line and the airport’s reporting line might mean valuable response time is lost when a security incident occurs. Training that does not lead to improvement in situational awareness may mean that airport staff learn how to report a security incident, but that unconscious ways of thinking and behaving mean that they do not actually use the reporting line when they observe a suspicious character waiting in a coffee shop.

There might also be opportunities here, though. Perhaps the airline has some lessons to share with you, which you can incorporate into your approach. Perhaps the hotel could influence your thinking on customer experience, and challenge you to think creatively about how to approach security from customer-centric perspective. The messaging that you develop might be useful in the airport terminal, for example. If you can find ways to describe benefit for situational awareness training, as frustrating as it might initially be, perhaps you will find it easier to convince other people in the airport community (e.g., tenant businesses) to spend some of their own money on the training.

## How might you respond?

When different micro-cultures and organizational systems collide, these sorts of interactions are very normal. In almost all instances, they come from a position of each stakeholder group wanting to do what they think is best.

Each situation is unique, and there is no single way to respond every time. There are, however, change management principles that you might use to assist you. Ask yourself the following questions:



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Case study – Implementing SeMS across differing levels of readiness and maturity

### 1 Have I taken the time to really understand what is important to this particular stakeholder?

Have I really listened? For example, have I really thought about what it might mean for the hotel if they accidentally embarrass a guest, who then writes a terrible review on their website? With the airline hub, they have invested large amounts of money in a reporting system that is working really well for them, and allows them to collate data from their places of operation all around the country. This is really valuable to them and in the case of the procurement and finance people, saving as much money as possible really is a big part of their role. They might need to answer questions on why they allowed your training to be approved, even though they do not know how to articulate the benefits that the training might bring.

### 2 If you really understand the viewpoints of your stakeholders, are there ways to frame your suggestions that speak to what is important to them?

Sometimes you need to reframe your messages:

- For your procurement and finance people, can you explain the effectiveness of situational awareness training, and can you show how much money the airport would stand to lose if an incident occurred? Can you present them with case studies from other incidents in other airports?
- For the hotel, can you work together with the General Manager to identify ways in which reporting suspicious behavior can be viewed as caring for customers? Perhaps you can put some thought into how incidents of suspicious behavior might be dealt with specifically in the hotel, in a way that comes across well to customers.
- For the airline, perhaps you look at ways to regularly share information across your two systems. Perhaps you can put in place specific protocols that mean your reporting line is instantly notified when something is reported in your airport, using the airline's reporting number.

Sometimes there might be prevailing myths, particularly among certain people in stakeholder groups, that influence how people receive what you are saying. For example, perhaps there is a myth at the hotel that when you use a reporting line, armed police will always arrive and take charge in a very aggressive way. If you uncover this myth, you can make sure to directly send a different message of what happens when suspicious activity is reported.

### 3 Can you find people of influence, who stakeholder groups might listen to more easily than yourself? For example:

- For the airline, can you work with their own Training Manager to do the security training needs assessment rather than imposing your own assessors on them?
- For the hotel, can you have someone more senior within your airport interact with their General Manager, to take a bigger picture view of how an incident coming from the hotel could impact the profitability of all organizations operating on the airport footprint?
- For your procurement and finance people, if there was just one person who you could spend time building a relationship with, who would it be?



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Case study – Implementing SeMS across differing levels of readiness and maturity

Sometimes, your biggest champions can be people who at first seem to be your biggest detractors. If you can bring with you the people who carry the most influence in a system, then you are more likely to catalyze wider change.

In that light, you should not always recruit champions from people who naturally agree with you or who put themselves forward as wanting to be SeMS Champions. Consider spending time building positive relationships with people who might not initially agree with you, and see if over time they might start to see value in your approach.

### 4 Is this something that is critically important, where you simply have to get compliance as soon as possible, or can it take time to develop and mature?

If it is absolutely vital, then you might need to take a direct approach and have someone very senior work with you to push through changes. If you can take some time, you can choose to work with stakeholder groups who want to work with you, and in time trust that through observation, role modeling, and ongoing relationship building, you can encourage more to join you.

### 5 Is this a case where you are trying to force something that is not needed?

In the case of the airline hub, perhaps you simply agree to pursue your different SeMS approaches for now. Perhaps you continue to stay in touch and share best practices, but do not take it any further for the time being.

### 6 Is there anything about your own approach that you need to reconsider?

Are your expectations fair, reasonable, and possible? Or are you imposing something that does not add reasonable value to that stakeholder group even if you feel that it is something you would like to do?

### 7 Have you really provided adequate explanation, and have you made sure that you are doing what is within your influence to provide an enabling environment for the stakeholders you are asking to work with you?

Have you really looked at barriers and enablers for them, and done what you reasonably can to assist? For example, it is possible for security checks to result in slower queues, which in turn may lead to penalties for poor customer service. Consequently, adequate security checks may not happen properly during busy times. This issue needs to be addressed if security behavior is to change.

### 8 Remember that a single means of engaging or interacting is not enough.

You need repeated conversations, in different ways and at different times, to gradually build understanding between stakeholder groups.

### 9 System change takes time.

Depending on your particular airport, it is perfectly reasonable to expect change to take years. Five years would not be an unreasonable time frame, and this is if you are consistent and persistent in your approach.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Case study – Implementing SeMS across differing levels of readiness and maturity

---

**10 Stakeholder groups need feedback, both when it goes right and when it goes wrong. Make sure you publicize and celebrate successes.**

Pay attention to the feedback, incentive, and communication mechanisms that you put in place to maintain conversations with your stakeholders.

**11 When you encounter negative responses such as irritation, anger, confusion, disinterest, or suspicion, recognize that these are perfectly natural responses to being asked to do something new.**

Always communicate:

- The reason you are suggesting what you are suggesting.
- Point out how it benefits the person you are speaking to directly, as well as how it will be of wider benefit to the whole airport community.
- Ask open questions. Listen to the response. Acknowledge even negative emotions that you may wish you were not hearing!
- Ask for suggestions.

**12 Expect that when stakeholder groups take on new behaviors, tools, or processes, it might take some time for this to become consistent and there might be setbacks.**

Again, expect some moments of challenge and negative reaction; often this a sign that you are successfully shifting the old ways of doing things. The important thing is to keep communicating, persisting, feeding back, making sure that you are being fair and reasonable, and adjusting your approach as needed.



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices

## Author Acknowledgements

---

Thank you to the following organizations for their participation in the interviews and validation workshop in 2016-2017 and contribution to the Guidance development:

ABM Aviation

Burlington International Airport

DNATA ground handling

General Mitchell International Airport

New South Parking

Oakland International Airport

San Antonio International Airport

Norman Y. Mineta San Jose International Airport

Sarasota-Bradenton International Airport

United Airlines

University of Southern California

32BJ SEIU



1

Getting to know  
SeMS

2

Are you  
SeMS ready?

3

How to establish  
your SeMS

4

Appendices