IFALPA
The Global Voice of Pilots
Position
14POS16 24 October 2013

Security Management System (SeMS)

Introduction

SeMS may be defined as a formal, risk-driven method of integrating security into an organization. This methodology requires coordination of activities, responsibilities, practices, procedures, processes and resources (i.e. it has to be Systematic, Proactive and Explicit).

In more ordinary words, SeMS is a holistic approach to security striving to move from a classical (reactive) perspective to a more proactive and predictive one. It moves away from a "one size fits all" to a more tailored system. Still, restrictive baseline measures may be necessary, but flexibility should be allowed in the system to let it adapt itself to cope with the specific threats and security needs of an organization.

Operational decisions and planning should be consciously considered at every level of an organization at all times and every process in the organization has to be consistent with a predefined plan but it also must have capability to adapt to the ongoing environment.

An effort has to be made within corporations to connect all management systems in the organization to work in coordination with the others (SMS, QMS, EMS, OHSMS, etc.).

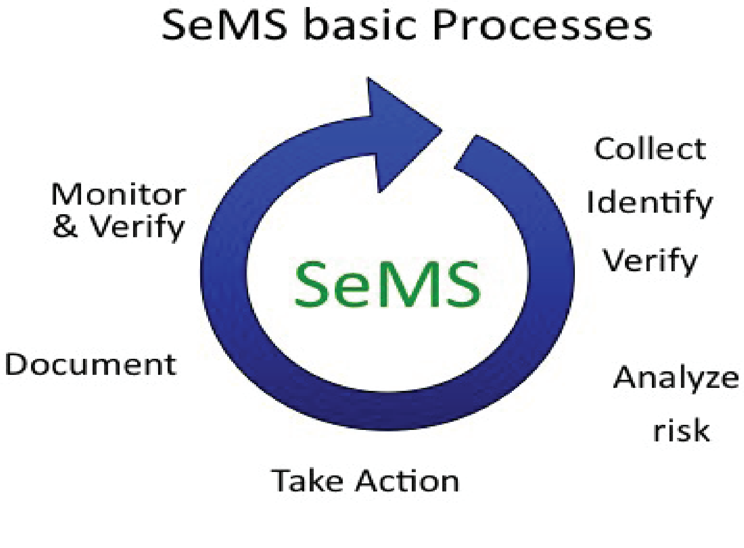

Figure 1: SeMS basic Processes

Management and state's role

In SeMS there are number of priorities. The first is to convince top management and top government officials about the importance and need to effectively apply SeMS in an organization, and that it would not work unless there is an explicit and strong support by both. This would allow implementation of an effective security culture from "top to bottom" and the necessary resources would be provided throughout the organization. Accountability of senior Management has to be established and a responsible person nominated within the organization.

SeMS should include a State's side e.g. regulatory requirements, oversight and definition of State's expected security performance, and an organizational side e.g. SeMS manual, self evaluation and defined level of security performance.

Threat and risk management

Measuring performance is one of the biggest challenges SeMS has to confront. That is why it is important to develop a good risk management system that could analyze the organization, measure its performance, define the risk and apply, if needed, the necessary mitigating measures.

SeMS requires the assessment of risk through a specific and structured methodology without allowing a subjective perception of reality to interfere. We may argue that there is always a subjective perspective in every analysis we make (at least in the ones humans do) but this will be kept to a minimum the more objective data is made available to qualified risk analysts.

Data collection and sharing of information

Robust risk assessment and management have to be developed within SeMS since this system will only be as strong as its capacity to acquire valid data to perform an adequate risk assessment.

Dissemination of security sensitive information is of paramount importance. Intelligence sharing methodologies within States and interested parties need to be coordinated since, in the past, it has been a key factor to prevent terrorist actions. This information should be delivered to pre-defined and selected parties in a need to know basis only.

AVSEC training and security culture

Security training and a good security culture (including just culture) are of paramount importance to achieve an acceptable level of security performance. National Training Programs must require that organization's training programs include, at minimum, recurrent security awareness training for all personnel that play a role in aviation security.

The effective implementation of a mandatory and/or voluntary confidential security reporting system is a necessary tool to collect data and other security information. Motivation of personnel is a key factor for maintaining the security of operations, and the effective implementation of reporting systems gives the right message to the personnel that aviation security is everyone's responsibility.

Organizations and states oversight (security assurance)

States must perform inspections, tests, audits, trials or a combination of procedures to evaluate the actual security performance of the system. This would indicate whether the reporting system works adequately. One of the basic principles of any management system is that it requires continuous reevaluation and, in this case, a security assurance process.

A global quality control and quality assurance evaluation of the organizations' and States' security performance has to be put in place in order to verify that it is kept within the predefined values.

In order to keep track of all processes, those would have to be constantly documented and be kept available for re-evaluation and oversight.

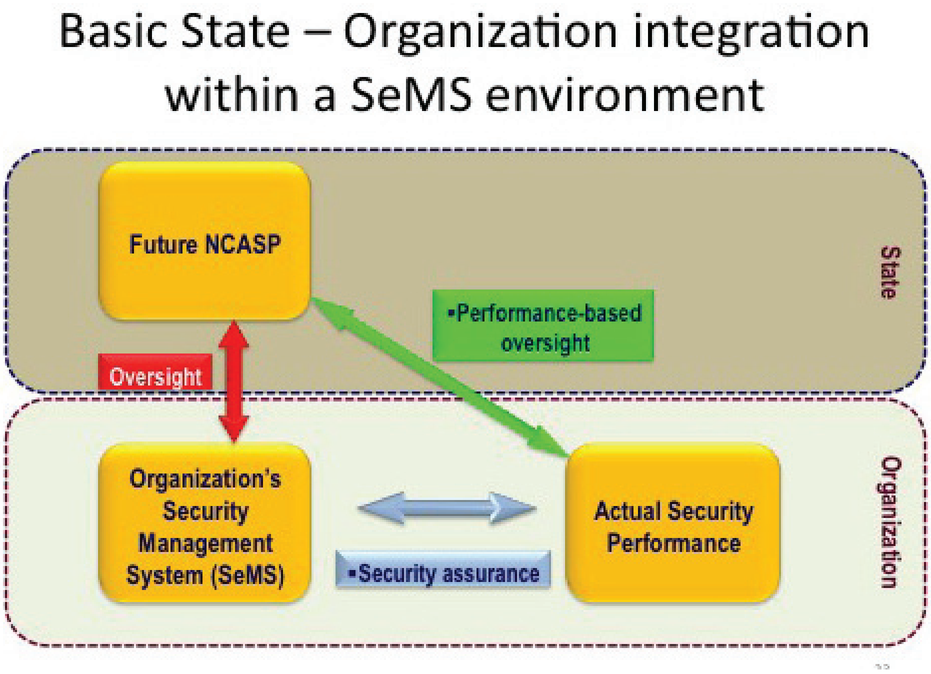
Basic State – Organization integration within a SeMS environment
Future NCASP
State
•Performance-based oversight
Oversight
Organization's Security Management System (SeMS)
•Security assurance
Actual Security Performance
Organization

Figure 2: Organization integration within a SeMS environment

Continuous improvement

The lack of registered security incidents is not a sign, by itself, of good security performance. SeMS requires all processes to be continuously reevaluated and improved.

Management of security incidents (Resilience)

A SeMS system strives to predict and prevent security mishaps at a very early stage. Additionally, States and organizations should develop contingency plans to manage the consequences of security incidents.

Cost

SeMS programs should be efficiently managed, using the available SeMS tools to streamline the security processes to contain costs. In any case, sufficient resources must be made available to ensure a satisfactory standard of security.

Conclusion

The implementation of SeMS is an improved way to address security issues. SeMS strives for a more outcome-focused, performance-based approach and a sustainable security model. Trial tests may be needed as proofs of concept of some of the previous statements to define procedures and best practices.

IFALPA provides this data for information only, in all cases pilots should follow their company's guidance and procedures. In the interests of flight safety, reproduction of this publication in whole or in part is encouraged. It may not be offered of sale or used commercially. All reprints must credit IFALPA.