



OUTLINE OF ICAO WORKSHOP

ON ENHANCING A POSITIVE SECURITY CULTURE

Introduction

A good security culture in an organization is an essential component of an effective, proactive and reactive security regime, which supports and maintains a risk-resilient structure that helps to manage effectively both insider and external threats and risks.

Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel within the organization. Security should be everyone's responsibility - from the ground up. Effective security culture is about:

- Recognizing that effective security culture is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or a burdensome expense.

Objectives

The objectives of the ICAO workshop are to:

- Explain the principles, importance and benefits of effective security culture.
- Present tools and best practices for the development of a strong security culture.
- Illustrate processes to use to develop behaviour change campaigns towards effective security culture.

Target Audience

The target audience of the workshop are:

- Middle managers of organizations (directly and not directly involved in aviation security to brief senior management);
- Security managers (or persons responsible to implement a security culture); and
- AVSEC instructors.

Note: Aspects of this workshop may be utilized in existing training materials targeted to other populations, such as senior management.

Duration: **4 days (classroom), 5 days (virtual)**

The workshop/s will be delivered through the ASTC network, ICAO offices (HQ/Regional) and industry training centres by subject-matter experts.

Content

I. Introduction

II. Understanding what is security culture

- a. What is security culture
- b. The importance of a strong security culture:
 - i. Aligning security to core business goals;
 - ii. Security as a core value; and
 - iii. Understanding the threat and risk environment, how it is managed and individuals' roles in that (mitigation).
- c. **Elements of a strong security culture:**
 - i. Positive work environments;
 - ii. Training;
 - iii. Leadership;
 - iv. Understanding the threat;
 - v. Vigilance;
 - vi. Reporting systems;
 - vii. Incident response;
 - viii. Information security; and
 - ix. Measures of effectiveness.
- d. **Embedding security behaviour change.**

III. Benefits of an effective security culture

- a. All risks mitigation (inc. insider and external threats).
- b. Engagement and responsibility on security issues (reporting suspicious activity).
- c. Levels of compliance with protective security measures increase:
 - i. The risk of security incidents and breaches is reduced by encouraging employees to think and act in more security-conscious ways (for example: deterrence effect- countering hostile reconnaissance).
- d. Employees are more likely to identify and report behaviours/activities of concern.
- e. Employees feel a greater sense of security.
- f. Security is improved without the need for a large expenditure.

IV. Implementation of a strong and an effective security culture

- a. Security Management Systems (SeMS).
- b. Project plan* and communications strategy.
- c. Steps towards implementing a strong security culture.
- d. Communication tools.
- e. Reporting tools - implementation of a Just Culture.
- f. Training, awareness and motivation.
- g. Change management.
- h. Evaluating impact.

V. Security culture exercise

The content, location, and number of exercises included in the security culture workshop are to be determined.

VI. Conclusion

*Understand your requirements. Define the aims and objectives of a security culture improvement plan. Create the security culture mission statement and strategy. Develop an implementation plan. Evaluate the impact.