International Civil Aviation Organization

WORKING PAPER

A41-WP/421[1]
TE/161
2/8/22

ASSEMBLY — 41ST SESSION

TECHNICAL COMMISSION

Agenda Item 33: Other issues to be considered by the Technical Commission

INFORMATION SECURITY MANAGEMENT SYSTEM APPLIED TO AIR NAVIGATION SERVICES IN VENEZUELA

(Presented by Venezuela (Bolivarian Republic of), supported by Costa Rica, Dominican Republic and Panama[2])

EXECUTIVE SUMMARY

The purpose of this working paper is to present a summary of advances in the development and application of the Information Security Management System (ISMS) in Air Navigation Services (ANS), process and next steps planned.

Action: The Assembly is invited to:
a) take note of the information provided;
b) disseminate initiatives on risk analysis development and, concomitantly, on ISMS development; and
c) examine the establishment of a sub-group to share knowledge, system performance and experience of ISMS implementation applied to ANS.

Strategic Objectives:	This working paper relates to Strategic Objectives: Safety Air Navigation Capacity and Efficiency
Financial implications:	
References:	Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference* (4.9.1- 4.9.2) Doc 10075, *Assembly Resolutions in Force (as of 6 October 2016)* (Item A39-19, pp. 91 to 93) CSA 43-107 and 45-107 National Civil Aviation Safety Plan (PNSAC) ISO 27000 series Venezuelan Laws and Regulations

[1] Spanish version provided by Venezuela (Bolivarian Republic of).
[2] Member States of the Latin American Civil Aviation Commission (LACAC)

1. INTRODUCTION

1.1 Pursuant to ICAO's recommendations in Annex 17 and following other good practices established in the ISO 27000 series for the implementation, maintenance and management of the Information Security Management System (ISMS), the evaluation of information and communication technology systems and of critical data used in ANS has begun in order to determine risks and the measures that must be taken in view of the specific characteristics and location of each one. It is thus known which elements are critical and where gaps are found, so that appropriate actions can be taken to prevent them from being exploited.

1.2 As part of the development of ISMS, a task force comprising representatives of each technical operational area (radar, communication, radio navigation aids and aeronautical messaging) was established to identify any/possible vulnerabilities and discuss best practices in order to reduce them and thus avoid incidents. To those ends, knowledge was exchanged and study panels were convened on capacity-building in the fields of networks and cybersecurity.

2. DISCUSSION

2.1 As a fundamental aspect of an ISMS, a culture of cybersecurity adapted to the systems of Air Navigation Services can emerge concomitantly with technical risks analysis conducted not only on the basis of hardware failures, but also possible system attacks, owing to digitalization and the integration of systems and services.

2.2 Furthermore, it is very important to draw on the Services' human resources (telecommunication, computer, electronics and other engineers), who must be stand ready to develop, improve and study cybersecurity measures adapted to the services. The task force must re-evaluate many safety policies to determine which ones are secure and which ones should be implemented in order to improve extant policies step by step.

2.3 The panels should determine the importance of conducting awareness-raising campaigns on cybersecurity (seminars, infographics, etc.) not only for technical personnel, but also for system users. This will further the establishment of a culture of cybersecurity which will ensure that technical and operational work teams are aware of new existing risks.

2.4 The ultimate goal of ISMS development is to pave the way for the establishment of a cybersecurity unit administered by ANS system specialists, who have undergone training and capacity-building in that area of knowledge. Its work team would lead in support and guidance in system cybersecurity matters when the systems begin to open doors to other networks.

2.5 One of the first steps that must be taken concerns the appointment of an Information and Communication Technology (ICT) manager, who will be tasked with forming the work team and collecting the necessary information on ISMS development and on documents to be produced. It is important to point out, however, that the success of actual applicability of the above-mentioned points lies in active teamwork involving senior ANS managers, maintenance managers, technical system specialists and the ITC manager.

2.6 The ISMS presentation must be accompanied by a cybersecurity campaign for the technical, operational and administrative personnel of Air Navigation Services.

2.7 Another important factor concerns provision, after processes and procedures have been established, for the production of simulated scenarios in which possible attacks can be replicated, thus providing opportunities for technicians to learn, experiment and apply the necessary security measures for impact avoidance or minimization. This will be done in a safe environment, isolated from the systems.

3. CONCLUSION

3.1 ISMS development entails recognition of the criticality of each area so that resources and efforts can be channelled appropriately and well directed as a basis for service continuity.

3.2 Risk analyses lead to recognition of vulnerabilities not only in technical, but also inhuman/operational aspects and, for that reason, it is considered important that they be performed. The results obtained can be used to determine latent risks and better measures for conducting such analyses basically for each service or asset.

3.3 The formation of a multidisciplinary group of ANS professionals is crucial to the transfer of knowledge, raising awareness and implementation of adequate safety policies, with emphasis on risk minimization. Moreover, awareness-raising campaigns will give rise to cybersecurity education, as it affects not only the institution/business but also daily life.

3.4 The formation of regional/international groups on cybersecurity will generate support and information on the experience of States, owing to the exchange of information on hardware procurement, cybersecurity service providers, vulnerabilities identified and means of channelling them. At a time when cybersecurity attacks are increasing daily, it is considered to be an important opportunity for growth in this area and for stronger ties of cooperation and mutual assistance among States.

— END —