International Civil Aviation Organization
North American, Central American and Caribbean Office

WORKING PAPER

NAM/CAR/CATC/WG/8 — WP/03
17/05/24

Eighth NAM/CAR Civil Aviation Training Centres Working Group Meeting (NAM/CAR/CATC/WG/8)
Port of Spain, Trinidad and Tobago, 12 to 14 June 2024

Agenda Item 11: Other Business

PREPARATION OF AN AVIATION SECURITY RISK MANAGEMENT TRAINING

(Presented by Dominican Republic)

EXECUTIVE SUMMARY

This paper raises the need to promote the development of initial and periodic training on cybersecurity risk management for all personnel who manage and install critical information technology systems and perform maintenance tasks. With the support of ICAO, the aim is to develop Risk Management training where training centres can have a unified idea on the issue of acts of unlawful interference through cyberattacks.

Action:	To prepare an aviation security risk management training, addressed to personnel using in their work technological means with the capacity of remote work and risk management handling. The suggested actions are contained on paragraph 3, items 3.1 and 3.2.
Strategic Objectives:	• Safety • Security & Facilitation
References:	• Annex 17 – *Aviation Security*, Safeguarding International Civil Aviation against Acts of Unlawful Interference, Twelfth Edition, July 2022 • Doc 8973 – Restricted – Aviation Security Manual • Cybersecurity in Aviation Strategy – ICAO (2019)

1. Introduction

1.1 The civil aviation industry depends on the availability of information, communication and control systems, as well as on the integrity and confidentiality of data. It is recommended to identify critical systems of technology and to apply protection measures based on risk evaluations in order to mitigate vulnerabilities and provide a response whenever an incident occurs. Cyberattack threats are evolving in different areas, especially for civil aviation, whether to subtract or destroy information or other critical motives that could affect the world. The trustworthiness, integrity and availability of all aviation systems are the main purpose of the aviation industry.

2. Analysis

2.1 With the increase of air transport capacity for 2030, it is a challenge for ICAO to be prepared to provide a timely and efficient response to avoid insecurity and lack of trust in the public who uses this means of transportation.

2.2 Information systems, computer programmes, among other media, are the most vulnerable due to the increasing volume of information management through computer systems and possible cyber threats caused by data volumes that could be generated. Technology is essential for aviation, but it also demands to over protect systems against possible attacks and to identify vulnerabilities to be used to commit acts of unlawful interference.

2.3 Every day, the integrity of information is more vulnerable to sophisticated hackers and to new technological tools that represent one of the greatest threats faced by civil aviation.

2.4 Standard 4.9.1 of the Twelfth Edition of Annex 17 to the Convention on International Civil Aviation states:

> *"Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference."*

2.5 Recommendation 4.9.2 of the Twelfth Edition of Annex 17 to the Convention on International Civil Aviation states:

> *"Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities."*

2.6 ICAO provides guidance in chapter 18 of Doc 8973 – Aviation Security Manual, 13th Edition, regarding cyberthreats against information technology critical systems and against aeronautical communications in paragraphs 18.1 and 18.2.

3. Suggested Actions

3.1 It is suggested to elaborate a risk management training for all personnel who uses, handles or installs critical information technology systems and who performs maintenance of tasks.

3.2 It is suggested to incorporate this cybersecurity risk management training within the National Civil Aviation Security Training Programme (NCASTP).

— END —