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

WORKING PAPER

NACC/DCA/14 — WP/19
15/05/26

**Fourteenth Meeting of the North American, Central American and Caribbean Directors of Civil Aviation (NACC/DCA/14)**

St. George's, Antigua and Barbuda, 1 to 5 June 2026

---

**Agenda Item 6:** **Seamless and Interoperable Air Navigation Services (ANS) that are Fit for the Future**

# STRENGTHENING CYBERSECURITY IN CENTRAL AMERICAN CIVIL AVIATION

(Presented by COCESNA)

**EXECUTIVE SUMMARY**

Cybersecurity in civil aviation has become a fundamental pillar for ensuring operational safety and the efficiency of air navigation. The industry currently faces a dynamic environment with constantly evolving cyber threats, which requires a strategic and coordinated approach to protect critical infrastructure.

This working paper presents a preliminary assessment of the cybersecurity posture of the Central American Corporation for Air Navigation Services (COCESNA) and the need to implement a regulatory framework based on NIST standards and the corresponding measures and controls to strengthen the Corporation at the corporate level, as well as the impact these measures may have on operational safety in the Central American Region.

It also addresses the need to have technical cooperation mechanisms in place that make it possible to sustain, with a long-term vision, the corporate implementation of a cybersecurity regulatory framework based on ICAO standards, NIST standard, ISO 27000 Information Security and ISO 31000 Risk Management, structured around three fundamental pillars: strengthening institutional processes, incorporating technological capabilities and controls, and developing human talent through training, specialisation and continuous awareness-raising.

| | |
|---|---|
| Action: | Under Section 5. |
| *Strategic Objectives:* | • All flights are safe and secure.<br>• Seamless, accessible, and reliable mobility |
| *References:* | • NIST Regulatory Framework |

**1.** Introduction

1.1. COCESNA received a technical assistance mission carried out by the ICAO NACC Regional Office, which took place in Tegucigalpa, Honduras, from 13 to 17 October 2025, and took as its main reference the ICAO guidelines and frameworks, especially Doc. 9985, Doc. 10213, Annexes 17 and 19, as well as international standards such as ISO/IEC 27001 and ISO 22301. The work plan included a training workshop on cybersecurity principles, regulations and best practices applied to CNS/ATM systems; an on-site technical visit to COCESNA's CNS/ATM and radar facilities; and a technical and operational assessment based on document review, interviews, direct observations and preliminary analysis of the existing controls, with emphasis on vulnerabilities, incident management, mitigation and alignment with ICAO's global cybersecurity framework.

1.2. The assessment showed that COCESNA has significant strengths, particularly in ATM security documentation, corporate risk management, basic network segmentation, and physical and logical control measures already in place. However, it also identified areas requiring action and strengthening, which COCESNA is in fact already proactively considering in its 2026–2030 Strategic Plan, which will strengthen the complete and sustainable integration of cybersecurity into air navigation services, including the consolidation of a formal governance framework with corporate-level scope, improvements in the definition of roles and responsibilities, greater involvement of the operational and OT areas in risk management, expansion and automation of the inventory of critical assets, strengthening of supplier management, and improvement of monitoring, vulnerability management, incident response plans and business continuity.

1.3. Taken together, the results show a positive foundation, but given that we are operating in a highly evolutionary, dynamic environment with major challenges, this leads to the implementation of objectives, strategies and actions for the ongoing strengthening of cybersecurity management as a key element for operational safety and continuity in the provision of services.

1.4. In this context, cybersecurity has been incorporated into COCESNA's 2026–2030 Strategic Plan (PEC) through strategic objectives, specific objectives and annual operational plans to be developed throughout the period, establishing a series of activities aimed at progressively strengthening corporate capabilities. These actions are structured around three fundamental pillars: strengthening processes (regulatory framework), incorporating cybersecurity technology and controls, and developing human talent through training, specialisation, and continuous awareness-raising, with the purpose of consolidating a more resilient, sustainable posture aligned with international best practices.

**2. IMPLEMENTATION OF CYBERSECURITY IN COCESNA**

2.1 As a result of the technical assistance mission carried out by the ICAO NACC Regional Office, COCESNA was recommended to move towards a structured, corporate and risk-based approach through the implementation of an Information Security Management System (ISMS) aligned with the NIST, ISO/IEC 27001, ISO 31000, ISO 22301 standards and ICAO Doc. 9985.

2.2 Within its 2026–2030 Strategic Plan, COCESNA has established a series of initiatives described below:

a. Comprehensive Assessment and Diagnosis of Cybersecurity Controls: This includes conducting a comprehensive assessment and diagnosis of cybersecurity controls based on the NIST standard. It includes the development of assessment instruments, the execution of the diagnosis, detailed gap analysis, and the definition of improvement action plans. In addition, it includes the full inventory of technological assets, their classification according to criticality and sensitivity level, as well as the registration of key services and their dependencies in the Configuration Management Database (CMDB). This assessment will be conducted cyclically throughout the planning/execution period, establishing a baseline in the first year that will make it possible to measure the evolution of control compliance.

b. Cybersecurity Governance Framework: The purpose of this initiative is to establish and maintain a robust corporate cybersecurity governance framework. It contemplates validation of the regulatory framework and includes the progressive development of specific instructions for Information Technology (IT) and Operational Technology (OT) environments, ensuring that the Corporation has up-to-date regulatory documentation aligned with international best practices.

c. Continuous Cybersecurity Monitoring: This initiative focuses on implementing solutions, services, systems, methodologies, and technologies that enable continuous monitoring of the Corporation's cybersecurity posture. The central component is the implementation and permanent operation of the Cybersecurity Operations Centre (SOC), for which COCESNA has already launched this service into production as of 16 March 2026, which is highly positive for strengthening monitoring capabilities and specialised external response to cybersecurity contingencies, thereby reinforcing uninterrupted surveillance of the technological infrastructure, the timely detection of threats and an effective response to security incidents. In addition, technological measures, controls, and improvement actions identified from cybersecurity assessments will be progressively implemented, continuously strengthening the Corporation's defence capabilities.

d. Cybersecurity Training and Awareness: This initiative reflects COCESNA's recognition that the human factor constitutes a critical element in the corporate cybersecurity posture and includes the development and implementation of comprehensive training and awareness programmes. It includes cybersecurity induction for new staff, the identification of training needs and definition of training plans, the execution of ongoing awareness campaigns to keep staff up to date on cybersecurity issues, as well as the implementation of basic technical training for all corporate staff through self-paced courses on e-learning platforms developed with ICCAE, together with specialised training for key personnel. The objective is to develop a robust cybersecurity culture at all levels of the Corporation and significantly reduce the risk associated with human behaviour.

## 3. TECHNICAL COOPERATION MECHANISMS}

3.1 The implementation and sustainability of a NIST-based cybersecurity framework require a continuous technical, organisational, and financial effort. Its development demands recurring investments aimed at strengthening processes, updating, and renewing technological capabilities, including the procurement of specialised monitoring and response services, as well as the training, education, and continuous awareness-raising of human talent to maintain a cybersecurity culture.

3.2 In this context, it is necessary to promote technical cooperation mechanisms and financial support that help sustain this strengthening process. Technical support, such as that provided through ICAO assistance missions, together with external support resources, can facilitate gradual and sustainable implementation.

3.3 Strengthening COCESNA's cybersecurity capabilities will bring direct benefits to the safety, resilience, and continuity of air navigation services in Central America. Likewise, the experience, lessons learned and capabilities developed at the corporate level may constitute a useful reference for their subsequent adaptation and replicability in the Civil Aviation Authorities of the region, favouring a more harmonised and progressive approach to regional aviation cybersecurity.

## 4. CONCLUSIONS

4.1 The preliminary assessment of COCESNA's cybersecurity posture shows relevant progress, but also aspects that COCESNA is already proactively managing in its 2026–2030 Strategic Plan in order to consolidate a corporate, structured and sustainable approach, underpinned by a regulatory framework based on the NIST standard and international best practices applicable to civil aviation (ISO 27000, ISO 31000, among others).

4.2 The incorporation of cybersecurity into COCESNA's 2026–2030 Strategic Plan (PEC), through strategic objectives, specific objectives and annual operational plans, constitutes an institutional basis for driving progressive and measurable strengthening across the three fundamental pillars: processes, technology, and human talent.

4.3 Given the continuous and costly nature of the implementation and sustainability of this framework, it is necessary to promote technical cooperation mechanisms, specialised assistance and financial support that make it possible to sustain over time the institutional capacities required for its operation and continuous improvement.

4.4 Strengthening COCESNA in cybersecurity matters will generate direct benefits for the safety, resilience, and continuity of air navigation services in Central America, and may also become a useful reference for its progressive adaptation within the Civil Aviation Authorities of the region.

4.5 In this regard, the present initiative represents an opportunity to move towards a more harmonised regional approach to aviation cybersecurity, in line with the guidelines and objectives promoted by ICAO for the protection of international civil aviation.

**5. SUGGESTED ACTIONS**

5.1 The Meeting is invited to:

a) support the implementation of a cybersecurity framework based on applicable standards, ICAO, ISO, NIST and complementary regulations, in response to the identified needs and its importance for the operational safety of civil aviation in Central America and the CAR Region.

b) support compliance with the initiatives incorporated into COCESNA's 2026–2030 Strategic Plan (PEC) and the annual operational plans, aimed at the progressive strengthening of processes, technology, and human talent in cybersecurity matters.

c) Provide (or arrange) technical cooperation and specialised assistance, including support missions and methodological guidance, to facilitate a gradual and sustainable implementation of the cybersecurity framework.

d) Manage and promote financial support that helps sustain the recurring investments required for specialised services, technological updating, and continuous staff training.

e) Support the capacities, experience and lessons learned derived from the strengthening of COCESNA so that they may serve as a reference for their progressive adaptation within the Civil Aviation Authorities of Central America, favouring a more harmonised regional approach to aviation cybersecurity throughout the region.

— END —