International Civil Aviation Organization
CAR/SAM Regional Planning and Implementation Group (GREPECAS)

WORKING PAPER

GREPECAS/23 — WP/5.7
14/01/26

Fifth GREPECAS–RASG-PA Joint Meeting (GREPECAS-RASG-PA/5) and Twenty-Third Meeting of the CAR/SAM Regional Planning and Implementation Group (GREPECAS/23)

Virtual Phase (Asynchronous, 19 January to 17 February 2026)
In-Person Phase (Mexico City, Mexico, 4 to 6 March 2026)

Agenda Item 5: Assembly 42nd Results; Matters Concerning Air Navigation Initiatives

CYBER RESILIENCE ENHANCEMENTS: THE ROLE OF CONTINGENCY PLANNING AND CYBER EXERCISES

(Presented by Brazil)

EXECUTIVE SUMMARY

This paper addresses the critical need for establishing robust contingency plans for civil aviation systems, in alignment with Pillar 6 (Incident Management and Emergency Planning) of the ICAO Aviation Cybersecurity Strategy. Furthermore, it explores the continuous improvement of these protocols through simulated cyberattack exercises, as advocated by Pillar 7 (Capacity Building, Training, and Cybersecurity Culture). By utilizing simulations based on real-world system vulnerabilities and facts already observed, organizations can significantly strengthen their defensive posture. The paper highlights the evolution of cyber threats within the aviation sector and underscores the fundamental synergy between practical exercises and contingency planning as essential drivers for institutional cyber resilience.

Action:	The Meeting is invited to: a) Promote the development of robust cyber incident management plans specifically tailored for critical aviation infrastructure; and b) Consider conducting recurring cyber simulations with integrated participation from government and industry partners in the CAR/SAM Region.
Strategic Objectives 2026-2050:	• Every flight is safe and secure • Aviation is environmentally sustainable • Aviation delivers seamless, accessible, and reliable mobility for all • No country left behind • The International Civil Aviation Convention and Other Treaties, Laws and Regulations Address All Challenges • The Economic Development of Air Transport Assures the Delivery of Economic Prosperity and Societal Well-Being for All
References:	• 42nd ICAO Assembly - WP/240 (Brazil). • Pillar 6 (Incident Management and Emergency Planning); and • Pillar 7 (Capacity Building, Training and Cybersecurity Culture) of ICAO Aviation Cybersecurity Strategy.

1. Introduction

1.1 In response to emerging risks and acknowledging the imperative for heightened protection of critical aviation assets, the ICAO Aviation Cybersecurity Strategy provides principles and actions structured across seven fundamental pillars, aimed at harmonizing resilience efforts throughout the international civil aviation actors. While technological modernization across South American and Caribbean airspace has enhanced operational efficiency, it has concurrently expanded the attack surface due to a profound dependency on digital infrastructures. This expansion is critical because cyber threats pose an escalating challenge to the civil aviation ecosystem, even within the CAR/SAM Region, where the high degree of systemic integration means that localized vulnerabilities can facilitate the rapid propagation of malware with transboundary consequences.

1.2 This working paper outlines the strategic initiatives undertaken by Brazil to bolster cyber resilience, specifically focusing on the integration of Pillar 6 (Incident Management and Emergency Planning) and Pillar 7 (Capacity Building, Training, and Cybersecurity Culture) of the ICAO Aviation Cybersecurity Strategy. By harmonizing these two pillars, the Brazilian civil aviation sector establishes a comprehensive and adaptive defense strategy for critical air traffic control assets. This approach transcends reactive measures, enabling a proactive stance that prioritizes the prevention and mitigation of threats, thereby safeguarding the enduring safety, security, and operational reliability of air transport in the CAR/SAM.

1.3 Ensuring minimal disruption to air traffic control, ground operations, and passenger services is the primary objective of the measures established under Pillar 6. This is achieved through robust recovery procedures and the implementation of clear, validated contingency plans designed for the immediate restoration of compromised systems and data. Essential to this approach is the availability of alternate systems, the maintenance of secure backups, and the execution of detailed, step-by-step recovery protocols.

1.4 A robust cybersecurity culture is fundamental to Pillar 7, ensuring that every individual—from air traffic controllers to ground maintenance staff—recognizes their position as a vital first line of defense. By addressing awareness and training for all stakeholders within the air traffic control environment, this pillar seeks to stimulate the training of personnel to understand their specific roles in incident response and the maintenance of a secure operational setting. Furthermore, it emphasizes the necessity of continuous learning and adaptation in response to an ever-evolving threat landscape. This commitment ensures that organizational readiness remains proactive rather than complacent, requiring constant improvement and the integration of updated cybersecurity technologies and strategies.

1.5 To contribute to a more secure and resilient global aviation ecosystem, it is essential to enhance collaboration between civil aviation cybersecurity authorities and other stakeholders through these principles. Thus, they establish a robust environment where contingency plans serve as the means to address malicious actions and respond to cyberattacks. The plans should address coordination among all actors, highlighting the critical requirements for implementing response actions, and detailing the mechanisms available to restore normal operations following a system compromise.

2. Analysis

2.1 In alignment with ICAO's cybersecurity strategy and its specific pillars, DECEA has been conducting training exercises for incident response teams to strengthen the resilience of the Brazilian airspace control system against escalating cyber threats. These exercises serve a dual purpose: they provide essential training for personnel from airspace control units and facilitate the identification of cybersecurity gaps emerging from the complex integration of air traffic control systems and applications.

The findings from these simulations are meticulously documented in reports, which are then utilized by the teams responsible for refining system security and updating contingency plans. Through these measures, Brazil continues to reflect international best practices in maintaining a secure operational environment.

2.2 To ensure a more accurate assessment and extract effective improvements for contingency plans and specific system gaps, each simulated situation is designed to mirror real-world occurrences, thereby closely replicating actual scenarios. This reliability is obtained and maintained through the involvement of system maintenance experts, who provide the necessary technical details to ground each exercise. As a result, the training actions allow for a precise evaluation of the adopted response measures, facilitating an accurate assessment of the environment and enabling the identification of necessary refinements for each individual system and the extraction of effective improvements for contingency plans.

2.3 In accordance with international standards such as ISO/IEC 27031, contingency plans are developed and carefully adjusted to address local specificities. This integration of global standards with the unique requirements of each site makes it possible to aggregate specific functional details within their respective plans. Consequently, even during a cyberattack, critical functionalities are preserved, and a controlled environment is maintained, ensuring a minimum operational continuity.

2.4 Minimizing system unavailability and the resulting impact on air transport users is the primary goal of the coordination and response actions described in the plans. The documentation details all information required to direct the reestablishment of system functionalities across different levels of air traffic control. These contingency plans, associated with each critical system in the Brazilian airspace control network, are based on the ICAO cybersecurity pillar concerning incident management and emergency planning. By identifying the various actors involved and their necessary coordination, the document provides a comprehensive basis for maintaining operational continuity.

2.5 By participating in the Brazilian national cybersecurity exercise, DECEA ensures that its contingency plans are consistently updated to counter emerging daily threats through a vital exchange of inter-sectoral expertise. This high-level involvement allows DECEA to contribute specialized airspace control knowledge to national security while integrating critical resilience insights from other strategic sectors into the refinement of aviation security measures. Building on this successful model of protecting critical infrastructure, Brazil urges ICAO CAR/SAM Region Member States and the aviation industry to organize similar collaborative exercises that unite government and industry experts. By using these platforms to share best practices, train incident response specialists, and develop more reliable contingency plans, the international community can effectively strengthen the collective security posture of the global aviation sector.

3. Conclusion

3.1 Brazil's proactive stance in safeguarding its airspace is demonstrated by DECEA's initiatives, which align directly with Pillars 6 and 7 of the ICAO Aviation Cybersecurity Strategy. Recognizing that the intricate global network of civil aviation remains vulnerable to the ever-present challenge of cyber threats; these efforts prioritize the development of robust contingency plans. By adhering to international standards like ISO/IEC 27031 and tailoring them to local specificities, the sector ensures that resilience is built upon a foundation of both global best practices and specific operational needs.

3.2 The enhancement of cyber resilience is further driven by regular, realistic cyber exercises that foster a strong cybersecurity culture across all stakeholders while identifying vulnerabilities and

training incident response teams. Through the sharing of expertise and active collaboration in both national and international exercises, Brazil underscores the critical necessity for collective action. This commitment to continuous adaptation ensures that the global aviation ecosystem is better protected against the persistent and evolving nature of cyber risks.

4. Suggested actions

4.1 The Meeting are invited to:

a) Promote the development of robust cyber incident management plans specifically tailored for critical aviation infrastructure; and

b) consider conducting recurring cyber simulations with integrated participation from government and industry partners in the CAR/SAM Region.

— END —