



International Civil Aviation Organization

WORKING PAPER

A42-WP/438¹

EX/195

29/7/25

Revision No.1

22/8/25

English only

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

CYBERSECURITY GOVERNANCE IN THE CIVIL AVIATION SECTOR AND PRESENTATION OF THE SULTANATE OF OMAN'S EXPERIENCE IN THE UNIVERSAL SECURITY AUDIT PROGRAMME- CONTINUOUS MONITORING APPROACH (USAP-CMA)

(Presented by Oman)

EXECUTIVE SUMMARY

This paper highlights the importance of effective governance to protect the civil aviation sector against cyberattacks, being the foundation for strengthening coordination and communication with a view to countering cyberattacks in this vital sector.

Countering cyberattacks starts by developing a clear structure adopted by the Civil Aviation Authority (CAA), as the regulatory entity of the sector. The structure includes a division for regulation (legislation and oversight) and several divisions related to sections mandated with implementation across the sector.

The paper also highlights the importance of adherence to Annex 17 – *Aviation Security* requirements and ICAO guidance material on aviation cybersecurity, in order to achieve the highest compliance and thus enhance the global aviation security ecosystem.

ACTION: The Assembly is invited to:

- urge Member States to develop and adopt a uniform cybersecurity governance structure for the aviation sector, to ensure consistent compliance with international commitments, with a view to enhance the security and safety of global air transport against cyber attacks;
- encourage States to develop and coordinate the implementation of cybersecurity requirements through the unit or department responsible for compliance with the provisions of Annex 17 – *Aviation Security* of the Chicago Convention;
- encourage ICAO to develop guidance material in order to establish standardized cybersecurity governance; and
- take note of the experience of the Sultanate of Oman and benefit from the lessons learned from the *Universal Security Audit Programme - Continuous Monitoring Approach* (USAP-CMA).

*Strategic
Goals:*

This working paper relates to *Every Flight is Safe and Secure* Strategic Goal.

¹ Arabic version provided by Oman

<i>Financial implications:</i>	Implementation of the concepts proposed in this paper are subject to the availability of financial and human resources in Member States. The proposed concepts can also be included in the Global Aviation Security Plan (GASeP).
<i>References:</i>	Global Civil Aviation Policies Civil Aviation Strategy ICAO <i>Aviation Security Manual</i> (Doc 8973) Annex 17 – <i>Aviation Security</i> <i>Global Aviation Security Plan</i> (GASeP)

1. INTRODUCTION

1.1 The last two decades witnessed rapid developments in the use of modern information and technologies in civil aviation, with the aim of supporting automation, connectivity, interoperability and overall digital transformation. That trend has recently accelerated, especially at the operational level, leveraging the latest technological developments such as artificial intelligence, machine learning and big data analysis. Such digitization served to accelerate the implementation of new operational concepts on the ground and in the air, supporting the growth of the civil aviation sector while enhancing its safety, security, efficiency, capacity and sustainability.

1.2 Within the framework of the duties and responsibilities of the Civil Aviation Authority (CAA) in Oman, as stipulated in the Civil Aviation Law, and based on ICAO Standards and Recommended Practices (SARPs) designed to protect civil aviation against cyberattacks, CAA works in coordination with national authorities to develop and oversee the implementation of cybersecurity legislation, in accordance with the requirements of the National Civil Aviation Security Programme (NCASP), which reflects the relevant SARPs provided for in Annex 17 – *Aviation Security*, Civil Aviation Law in Oman and other national legislations that address cybersecurity.

1.3 National legislation is regularly developed and updated in accordance with the best practices that are compliant with provisions of Annex 17 of the Chicago Convention, SARPs on cybersecurity, the 2010 Beijing Convention, the 2010 Beijing Protocol, Assembly Resolutions A39-19, A40-10 and A41-19 on cybersecurity, ICAO Aviation Cybersecurity Strategy and Action Plan, as well as relevant guidance material and manuals; the most recent of which is the ICAO *Global Cyber Risk Considerations* (Doc 10213 – Restricted). National legislation as such constitutes the primary pillar relied upon in structuring the sector and assigning tasks and responsibilities among different entities in a manner conducive to protecting civil aviation against cyber threats.

1.4 Compliance aimed at achieving international commitment to civil aviation security and facilitation, by integrating them into national legislation, should follow a clear and organized administrative structure that ensures the development of comprehensive national legislation that helps operational staff mitigate risks and protect all civil aviation facilities against threats.

1.5 According to an ICAO report issued on December 31, 2024, 179 countries completed *Universal Security Audit Programme - Continuous Monitoring Approach* (USAP-CMA) on-site and document-based audits. The compliance index for Standard 4.9.1 showed a global average of 49%, which is due either to the lack of any requirement to identify critical infrastructure or the absence of effective cybersecurity measures.

2. CYBERSECURITY GOVERNANCE

2.1 It is important to ensure that there is a consensus as well as understanding of the roles and responsibilities related to cybersecurity, with the aim of ensuring international and national compliance in that regard, in terms of regulation and oversight. That in turn results in developing an efficient workflow designed to ensure that there is no overlap in competencies and responsibilities among departments and sections concerned with cybersecurity and fulfilling all requirements to protect civil aviation from cyber threats.

2.2 It is important for CAAs to pay great attention to the security of civil aviation, especially the length of its complex nature, in order to ensure an aviation environment that is secure, safe, regular, efficient, economic and protected through developing a comprehensive organizational governance structure and putting in place operational enablers that guard against cyber-attacks by leveraging the latest technologies.

2.3 This importance has become even more poignant given the sophistication and frequency of cyber threats and attacks around the world, their increasing complexity and various motives, such as organized crime, financial and political motives, etc. Added to that is the fact that institutions and businesses have become increasingly entrenched in the digital space through digital transformation processes and integration among entities.

3. CYBERSECURITY GOVERNANCE IN OMAN (THE NATIONAL LEVEL)

3.1 Regulating aviation cybersecurity is a responsibility that was assigned to the Aviation Security Department at the Civil Aviation Authority (CAA). As such, the Aviation Security Systems Division is responsible for developing and updating cybersecurity systems, the Oversight and Licensing Division is responsible for quality control activities (audit, inspection, follow-up, testing and investigation), and the Risk Assessment Division is responsible for assessing cyber risks.

3.2 Various departments across the sector are mandated with implementing all legislative requirements related to aviation cybersecurity.

4. THE OPERATIONAL LEVEL

4.1 Operational entities are responsible for complying with national requirements, developing standard operating procedures and implementing the necessary procedures to protect critical ICT systems and data used in civil aviation.

5. NATIONAL CIVIL AVIATION SECURITY AND FACILITATION COMMITTEE

5.1 The Oman National Civil Aviation Security and Facilitation Committee ensures the sustainability of civil aviation, in accordance with national legislation, programmes and plans and in line with ICAO SARPs.

5.2 It also makes strategic decisions that will enhance aviation security, facilitation and cybersecurity requirements.

5.3 Furthermore, it undertakes ongoing reviews and assessments of the effectiveness of security measures as threats continue to evolve and makes recommendations to modify relevant measures, based on threat information, technology development, aviation security techniques, and other factors that strike a balance between security and facilitation.

5.4 The National Civil Aviation Security and Facilitation Committee has approved setting up a technical/advisory committee on aviation cybersecurity.

6. NATIONAL LEGISLATION FOR CYBERSECURITY IN THE CIVIL AVIATION SECTOR

6.1 In addition to the National Civil Aviation Security Programme and the Civil Aviation Security and Facilitation Manual, the Omani CAA has issued documents related to cybersecurity, such as:

6.1.1 the Civil Aviation Cybersecurity Policy; and

6.1.2 the Civil Aviation Cybersecurity Guidance.

7. CYBERSECURITY AWARENESS

7.1 The Civil Aviation Authority in Oman ensures adequate awareness of cyber risks in civil aviation in Oman by drafting and disseminating awareness bulletins through various internal communication channels in the sector and by organizing and holding security awareness workshops to explain cyber threats and risks and means of guarding against them, as a way to mitigate cyber threats.

7.2 The CAA oversees aviation cybersecurity training and awareness material across the industry to ensure that the relevant material complies with national legislation as well as the approach endorsed by ICAO in this regard.

8. OMAN'S EXPERIENCE IN THE UNIVERSAL AVIATION SECURITY AUDIT PROGRAMME - CONTINUOUS MONITORING APPROACH (USAP-CMA)

8.1 The Civil Aviation Authority undertook optimal preparation and readiness for the USAP-CMA audit, a phase that included several steps, most notably:

- a) studying ICAO documents on cybersecurity and cyber resilience;
- b) developing, updating and adopting cybersecurity legislation and developing guidance material to support entities in implementing harmonized cybersecurity management frameworks, establishing a systematic approach to risk management, and assessing the maturity and effectiveness of those frameworks;

- c) disseminating national and international ICAO guidelines and training material to promote a cybersecurity culture;
- d) requiring operators to identify their critical ICT systems used in civil aviation;
- e) requiring operators to develop and implement measures to protect systems from unlawful interference;
- f) keeping abreast of and attending meetings held by ICAO working groups and teams to enhance governance for cybersecurity and cyber resilience;
- g) study and analyse meeting outcomes and team recommendations that facilitate the exchange of information and advocate for mobilizing resources and taking actions to achieve a holistic approach towards cybersecurity in civil aviation;
- h) establishing hubs for training sessions, briefings and workshops in across the sector; and
- i) launching the national programme "*Ertaqa 2*" (Evolution 2) to develop and implement effective working methods aimed at ensuring the implementation of the Global Aviation Security Programme (GASP) compliance procedures in Oman and develop solutions to meet the needs identified in the compliance plan, such as cooperation programmes with ICAO, providing the relevant expertise, and procuring the necessary technologies.

8.2 It has also conducted a simulation of an international audit to analyse and resolve identified gaps. This analysis of the aviation cybersecurity framework was conducted and compared to the one developed by ICAO. The framework covers the legal, organizational, operational and training aspects of cybersecurity in aviation. The analysis yielded some important recommendations, including:

- a) attracting competencies and expertise from among talents specialized in cybersecurity, aviation security and ICAO audits;
- b) appointing a cybersecurity expert and inspectors to act as a *liaison* with the CAA to ensure coordination with all entities in the industry;
- c) establishing dedicated working teams to implement recommendations and find practical solutions, including the *Ertaqa 2* team, which comprises several specialized teams that cover all nine audit areas;
- d) appointing a point of contact in each entity to coordinate with the CAA;
- e) supporting teams by meeting their logistical and technical needs;
- f) creating and providing tools to implement cybersecurity oversight and testing activities in the sector;
- g) setting up and implementing quality control and follow-up plans, as part of the activities of the operational team charged with the ICAO Audit;

- h) reviewing the results of quality control activities and submitting relevant reports and recommendations;
- i) undertaking support and capacity-building activities, workshops and cybersecurity awareness for all stakeholders in each entity;
- j) creating models and simulations to assess risks, identify critical systems and develop risk management procedures and contingency plans; and
- k) conducting simulated ICAO audits to determine the extent of compliance with ICAO's cybersecurity requirements.

8.3 Oman underwent an ICAO audit in the first quarter of 2025, passed the audit without any findings and achieved a 100% compliance rate with the provisions of ICAO Annex 17 and Cybersecurity SARPs.

9. LESSONS LEARNED FROM THE GAP ANALYSIS PHASE AND THE UNIVERSAL SECURITY AUDIT PROGRAMME CONTINUOUS MONITORING APPROACH (USAP-CMA)

9.1 It is crucial to emphasize the importance of international cooperation and effective governance and implement ICAO's provisions to ensure a uniform and coordinated cybersecurity approach across the world, which is critical as cybersecurity threats are cross-border in nature and can have far-reaching impacts on the safety and security of civil aviation.

9.2 Furthermore, the analysis covered the practical challenges faced by States and the aviation industry in implementing cybersecurity commitments, highlighting those challenges and the need for ongoing support, resources and training to help all parties strengthen their cybersecurity capabilities.

9.3 Overall, the analysis revealed that the ICAO Framework is a crucial step forward in addressing the evolving cybersecurity risks in civil aviation, by providing a comprehensive framework, guidance and support, as ICAO plays a vital role in protecting the safety and security of civil aviation.

— END —