International Civil Aviation Organization

WORKING PAPER

A41-WP/488[1]
EX/235
2/8/22

ASSEMBLY — 41ST SESSION

Agenda Item 15: Audit Programmes – Continuous Monitoring Approach

STRENGTHENING USAP-CMA AUDIT TEAMS FOR THE ASSESSMENT AND IMPLEMENTATION OF ANNEX 17 CYBERSECURITY REQUIREMENTS

(Presented by Venezuela (Bolivarian Republic of) and supported by Bolivia (Plurinational State of), Colombia, Costa Rica, Panama, Peru and Uruguay)[2]

EXECUTIVE SUMMARY

Under the Universal Security Audit Programme (USAP), States currently have guidelines that enable a general performance assessment of the State aviation security oversight system. This has made it possible to develop recommendations for improvement using common aviation security principles. Such an assessment is conducted by a team of auditors who ensure that these activities cover the critical elements of the aviation security oversight system in addition to the provisions of and level of compliance with the Annex 17 – *Aviation Security* Standards. Annex 17 specifies how to develop and implement measures for protecting information and communications technology systems, as well as critical data used for civil aviation purposes. With this in mind, audit teams need to be strengthened through the development of guidance or training material that will enable them to assess and implement the cybersecurity requirements set out in Annex 17.

Action: The Assembly is invited to:

a) note the information presented in this working paper; and
b) request that Council develop tools or training material to provide the USAP audit team with full guidance and training in cybersecurity so that the appointed groups can conduct an objective and technical assessment of the Protocol Questions (PQs) in line with the specialized aspects of cybersecurity in civil aviation.

Strategic Objectives:	This working paper relates to Strategic Objective: Security and Facilitation.
Financial implications:	We propose that the activities mentioned in this paper be conducted using resources available in the Regular Programme of the current triennium and/or through extra-budgetary contributions.
References:	Recommended Practice 4.9.1 of Annex 17 and USAP-CMA Protocol.

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

1. INTRODUCTION

1.1 The Universal Security Audit Programme (USAP) provides States with guidelines that enable a general performance assessment of the State aviation security oversight system. This has made it possible to develop recommendations for improvement using common aviation security principles. According to the USAP Continuous Monitoring Approach (USAP-CMA) Protocol, there are currently specific PQs (1345, 1350, 1360 and 3278) related to the assessment of general or basic aspects of developing and implementing measures for protecting information and communications technology systems, as well as critical data used for civil aviation purposes.

1.2 Such an assessment is conducted by a team of USAP auditors who ensure that such activities cover the critical elements of the aviation security oversight system as well as the provisions in and level of compliance with Annex 17 – *Aviation Security* Standards. Annex 17 includes the commitment of each State to assign responsibilities, establish national criteria for protecting systems associated with aviation operations through the implementation of protective measures, identify critical systems, carry out continuous monitoring, ensure detection, analysis, and response to cyberattacks, and to assess quality control activities conducted by the State in accordance with risk assessments.

2. ANALYSIS

2.1 Given the importance of the activities conducted under the USAP-CMA, it is important with respect to cybersecurity to ensure that the USAP audit team has guidance material that enables them to conduct an objective and technical assessment of the implementation of international standards, strategies and best practices developed and implemented by States for the identification and protection of critical information technology and communications systems against any interference that may compromise the safety, integrity or operation of the civil aviation system.

2.2 We currently have reference frameworks and existing practices at the global level that have enabled various organizations to manage efficiently and reduce the cybersecurity risks. Some examples include the standards of the ISO/IEC-2700 series designed to establish good practices for various aspects of information security management, continuous improvement and risk mitigation; the Control Objectives for Information Technologies (COBIT) Guide; the MAGERIT Risk Analysis and Management Methodology for Information Systems; and other international standards, guidelines and best practices.

2.3 The aforementioned reference documents represent significant progress in cooperation and global integration in cybersecurity, providing courses of action and benchmarks applicable and common to all types of critical infrastructure. Such benchmarks relate specifically to industry standards, guidelines and practices that make possible cybersecurity implementation and assessments, not only at the level of organization and documentation, but also with respect to operations and implementation.

2.4 With this in mind, we propose that standardized guidance material be developed to enable the creation of a reference framework that takes advantage of industry best practices and methodologies and the experiences of States in order to achieve a harmonized approach. This would not necessarily be a static document, but rather guidance material that would enable the team of USAP auditors to provide a technical and objective assessment of the level of compliance with the Standards, based on the specificities and needs of each State as presented in PQs 1345, 1350, 1355, 1360 and 3278.

2.5 The Appendix of this working paper presents suggested content model for the areas of knowledge and guidance material. The proposal is based on criteria taken from various standards,

guidelines and existing practices for information security management, continuous improvement and mitigation in organizations with internationally critical infrastructure. The Appendix highlights the following:

a) areas of knowledge and experience potentially necessary for assessing the cybersecurity measures implemented by States (according to the PQs); and

b) suggested content for drafting text or guidance material to enable the USAP audit team to assess and implement the cybersecurity requirements set out in Annex 17.

3. CONCLUSION

3.1 It is essential for the audit teams assigned to the implementation of the USAP-CMA to possess the tools and knowledge necessary for a precise, objective assessment of State compliance with the design, development and implementation of protection tasks for civil aviation cybersecurity in accordance with the requirements set out in the Standards and Recommended Practices of ICAO Annex 17 – *Aviation Security*.

— — — — — — — —

APPENDIX

SUGGESTED CONTENT FOR AREAS OF KNOWLEDGE AND GUIDANCE MATERIAL

a) Areas of knowledge and experience necessary for assessing the cybersecurity measures implemented by States

Knowledge of procedures and techniques for asset management and critical processes; identification and appraisal of technology assets or information associated with aviation; information security policies, procedures and measures; risk and incident management; management controls or safeguards that permit mitigation of cybersecurity findings; forensic, network, code, vulnerability and physical audits, web analysis, and others.

Technical capacity to assess protective measures by conducting tests, such as, for example: the collection, classification and identification of assets, scanning of services, vulnerability analysis and validation; operational test checks of the electrical supply system, equipment, dependent resources or systems when electrical system breaks down; testing of equipment for information system and IT platform management; tests of hardware, operating and infrastructure software and/or software applications; performance tests of the IT platform (under conditions of total interruption); test of the Internet backup service (disconnection from the primary channel, verification of secondary channel connection, load balancing, etc.); information recovery tests, and others.

b) Suggested content for drafting text or guidance material to enable the assessment and implementation of the cybersecurity requirements set out in Annex 17.

1. Guide to common critical processes in the civil aviation industry concerning airlines (management of passengers, baggage, cargo, ground assistance, flight dispatch, aircraft maintenance, among others); critical processes in airports (airport security, operations and airport infrastructure, management and airport emergencies, among others); critical processes in air transport management (voice communications, aeronautical messaging and radar data, air navigation, among others).

2. Standardized risk assessment methodology for the aviation sector that includes the determination of the context, policies and responsibilities, identification of operational processes, asset identification and appraisal, identification of vulnerabilities, and the identification of threats, their probability of occurrence, and estimation of impact (consequences).

3. Guide to controls or safeguards including network hardware management, management of authorized and unauthorized software, the base configuration for mobile devices, laptops, desktops, servers, continuous process of vulnerability identification and remediation, processes and tools for the identification, prevention and correction of the use and configuration of administrative privileges (networks/applications), the maintenance, monitoring and analysis of audit results, email and navigator protection procedures, management of ports, protocols and services in network devices; procedures based on appropriate methodologies and tools for backing up critical information and recovery tests; procedures for secure configurations of network devices (firewalls, routers and switches), perimeter defence; procedures and tools for data protection to prevent information loss, mitigate incidents, and ensure the confidentiality and integrity of sensitive information; procedures for incident management and response, and other controls.

— END —