INTERNATIONAL CIVIL AVIATION ORGANIZATION
AFI PLANNING AND IMPLEMENTATION REGIONAL GROUP (APIRG) PROJECT

DOMAIN : IIM (Infrastructure & Information Management)

Project Team Coordinator: **Côte d'Ivoire**

COM Project 5: Assessment of Air Navigation Services Cyber Resilience in AFI region

AFI Region	PROJECT DESCRIPTION	DP N° C	
Programme	**Title of the Project**	**Start**	**End**
Assessment of AFI Aeronautical Networks cyber security	Assessment of AFI Air Navigation Services Cyber Resilience **Project coordinador**: Côte d'Ivoire **Experts contributing to the project**: Côte d'Ivoire, Cameroon, Benin, Gambia, Ghana, Kenya, Nigeria, South Africa, Somalia, ASECNA, IATA, Cameroun, Madagascar, Somalia	01/08/2017	31/12/2023
Objectives	In the framework of the technologies Roadmap defined in the 6th edition of the GANP, - develop a global Cyber resilience framework over the AFI region for Air Navigation Services to prevent internal and external threats impacting availability, reliability, integrity, and continuity of Air Navigation Services - and assist States / organizations in implementing the AFI ANS Cyber resilience Framework		
Scope	The scope of the project includes: • assessment of the cyber threats on Air Navigation Services in Africa; • development of a cyber resilience framework[1] over the AFI region.		
Metrics	1) ANS Cyber resilience policies Number of AFI States/ ANSPs with an effective cyber resilience policy put in place % of AFI States/ ANSPs with an effective cyber policy put in place 2) ANS Cyber resilience training and awareness Number of Cyber resilience awareness campaign conducted by ANSPs/ CAAs in AFI Region		
Goals	Ensure that the Air Navigation Services are provided in compliance with ICAO SARPs, guidelines		

---

[1] This framework will be voluntary guidance, based on existing standards, guidelines, and practices for organizations to manage and reduce cybersecurity risk. It would assess all issues including the definition of common cyber threats, training & awareness, response, recovery performances, security studies, systematic process of cyber risk evaluation on all new systems, audits and controls.

AFI Region	PROJECT DESCRIPTION	DP N° C	
Programme	**Title of the Project**	**Start**	**End**
Strategy	All tasks will be carried out by COM/ IT experts nominated by AFI States participating in the project, led by the Project-Team Coordinator and under the supervision of the Project Facilitators (ROs/CNS, Dakar and Nairobi) through the IIM SG working methodology. Upon completion of the tasks, the results will be sent to the Project Facilitators as a final document for submission to, and if necessary, approval by the APIRG Projects Coordination Committee (APCC). The project relies on the following phases: • Project Definition (development of project documentation), • ANS cyber risk assessment (through survey) • Regulatory analysis • Development of AFI ANS Cyber safety and resilience framework • AFI ANS Cyber resilience awareness		
Justification	The air transport infrastructure is an attractive target for cyber-attacks due to its importance and prominence. The networks and systems, interconnecting the various ANSP are IP-based and are exposed at several levels to cyber-attacks. The cyber threats are real and can take several forms depending on the means of the hackers. Therefore, organizations must identify their critical information systems and implement appropriate cyber security measures in complement to existing cyber security objectives. There is a need for a cyber resilience approach for the aviation over the AFI region, which would assess all cyber issues.		
Related projects	All APIRG specifically projects related to: • **FICE B0/1 - Automated basic facility data exchange (AIDC)** • **COMI-B0** • **COMI-B1** • **COMS - B0** • **NAVS-B0** • **ASUR-B0**		

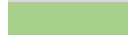| Project Deliverables	Relationship with the regional performance-Objectives (RPO) and ASBU modules	Responsible Party	Status of Implementation[2]	Date of Delivery	Comments
[D01] Project Description	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	31/12/2018	2022 update (alignment with 6th edition of GANP)
[D02] Project Organization Description	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	31/12/2018	2022 update
[D03] Terms of reference	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project coordinator	completed	30/06/2018	2022 update
[D04] Project linkage	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	30/09/2018	**2022 update**
[D05] Project questionnaire	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	30/09/2019	
[D06] Assessment of the current ANS cyber resilience and diagnostic of the potential threats to the safe provision of the air navigation service in the AFI region	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	30/12/2022	
[D07] Global cybersecurity framework for a secured operation of the AFI ANS systems, data and networks	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team	completed	30/12/2022	

---

[2] *Grey   Task not started yet*
Green   Activity being implemented as scheduled
Yellow   Activity started with some delay, but will be implemented on time
Red   Activity not implemented on time; mitigation measures are required

Project Deliverables	Relationship with the regional performance-Objectives (RPO) and ASBU modules	Responsible Party	Status of Implementation[2]	Date of Delivery	Comments
[D08][3] Teleconferences, Workshops/Seminars/webinars, working sessions (French and English) on global cyber resilience policy	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0 ASUR-B0	IIM SG/COM/Project 5 project team		31/12/2023	To be organized virtuall
[D09] Non exhaustive list of Aviation cybersecurity training offers	FICE B0/1 COMI-B0 COMI-B1 COMS - B0 NAVS-B0	IIM SG/COM/Project 5 project team	completed	28/06/2023	
Resources needed	• Adequate human resources to be appointed by States (experts from States) • Expertise in Aviation Cyber résilience • Funds to conduct Workshops, Seminars, and training on aviation cyber resilience (Air navigation services) • Likewise, participants must be given facilities to participate in teleconferences and coordination meetings. • Funds for meetings with project Team Members to assess the results and propose corrective actions.				

Grey Task not started yet
Green Activity being implemented as scheduled
Yellow Activity started with some delay, but will be implemented on time
Red Activity not implemented on time; mitigation measures are required

---

[3] Objectives:

Working Sessions are an essential tool to:

• Discuss with main African Stakeholders about key essential aspects of Cyber resilience in Aviation
• Network people and contribute to build capacity in Cybersecurity in aviation
• Deliver valuable information to decision makers about Cyber safety and cyber resilience
• Gather best practices from other regional initiatives on Cyberspace issues for Aviation

There is a need for ICAO and Designated Experts to conduct Technical workshops to support the development of the project