# "AFI Air Navigation Services Cyber safety and resilience assessment"

*IIM SG COM 5 Project Status Report*

**Third Meeting of the APIRG IIM/SG, 12-14 October 2020**

**Presented by: Côte d'Ivoire**
*(Sandrine GNASSOU)*

**AGENDA**

**1** **Introduction**

**2** **Discussion** ........................ 2.1 Scope
2.2 Actions conducted
2.3 Challenges
2.4 The way Forward

**3** **Action by the Meeting** .......
3.1 The meeting is invited to..
3.2 Draft Conclusion/Decision

## Attacks on Aviation are happening…

OVER **60 CYBER-ATTACKS** ON AVIATION SINCE JANUARY 2019*

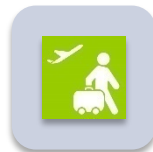THE AVERAGE COST OF EACH ATTACK IS **€ 1,000,000**
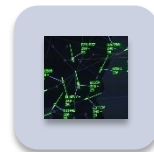
AVIATION WILL NOT EVER BE **100%** CYBER PROOF …

POTENTIAL **TARGETS** IN AVIATION

AIRPORT

AIRCRAFT

AIRLINES

AIR TRAFFIC MANAGEMENT/ ANS

**IIM SG COM 5 project is addressing AFI ANS cyber safety & resilience**

## Project Objectives

- To identify cyber threats on Air Navigation Services in Africa

- To assess current cyber resilience of Air Navigation Services in AFI region

- To develop a cyber safety and resilience framework for Air Navigation Services

## Project Members

*AIS, CNS experts, Cybersecurity and ICT experts from :*

- Benin
- Côte d'Ivoire
- Gambia
- Ghana
- Kenya
- Nigeria
- Somalia
- South Africa

ASECNA

ATNS

IATA

**IIM/SG/3- AI 4 – WP/04B.5**

# 2. DISCUSSION

2.1 Scope

2.2 Actions conducted *(project key achievements)*

2.3 Challenges

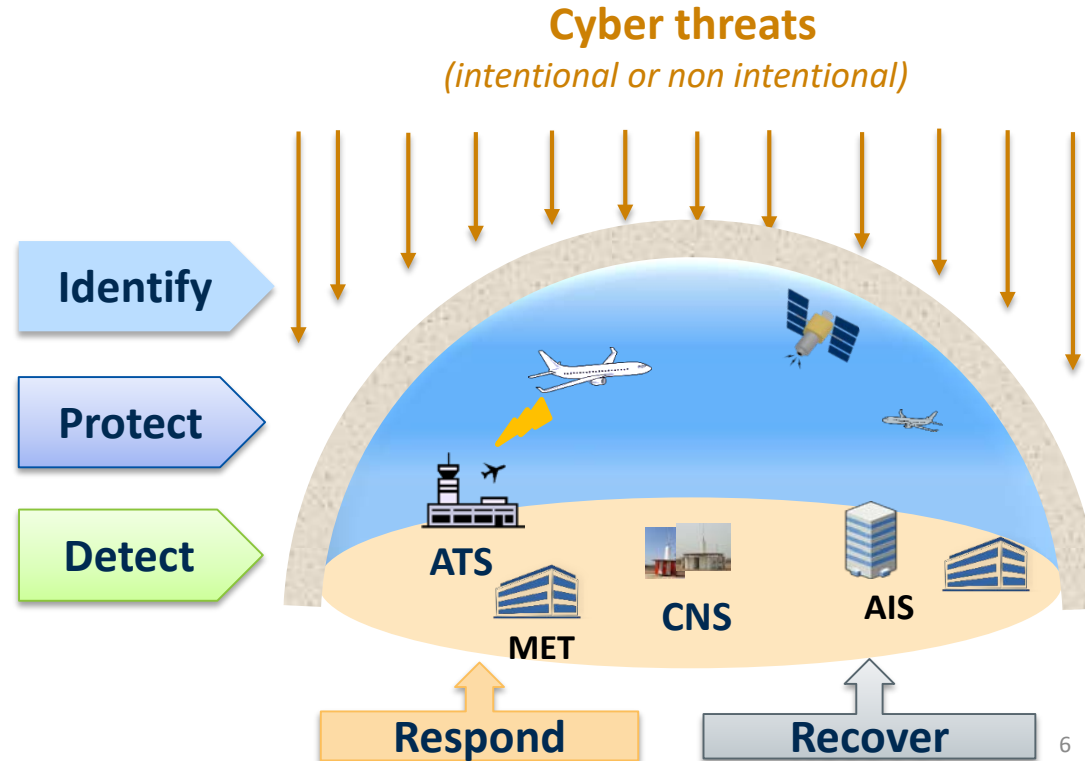2.4 The way Forward *(Project Upcoming Tasks and Milestones)*

# 2.1 Scope

## How can ANS be resilient to cyber threat?

**Cyber resilience**

- an organisation ability to continuously deliver the intended outcome despite adverse cyber events.

- Is a measure of how well an organization can operate its business during a data breach or cyber attack

**Cyber threats**
*(intentional or non intentional)*

Identify

Protect

Detect

ATS
MET
CNS
AIS

Respond

Recover

6

**75%** Project tasks completed

# 2.2 Actions conducted *(Project phases)*

| Project Definition | ANS cyber risk assessment | Regulatory analysis | AFI ANS Cyber safety and resilience framework | Formal Approval |
|---|---|---|---|---|

- Project Scope, Terms of Reference, ✓
- Project Description, organization and linkages with other IIM Projects ✓

- Project baseline questionnaire (to be sent to AFI states) ⏳
- List of ANS critical assets and data used in AFI region ✓
- Potential Cyber threats to ANS ✓

Analysis of existing cybersecurity and cyber resilience frameworks and guidelines *(ISO 27000 series, NIST framework, ICAO thrust framework, Aviation Cybersecurity Strategy)* ✓

Development by the project team (project internal validation) ✓

Review by IIM chairman and Secretariat ⏳

- Submission to APIRG Review and validation
- Update (if needed)
- Promotion of the framework

7

**AFI ANS Cyber resilience Assessment**
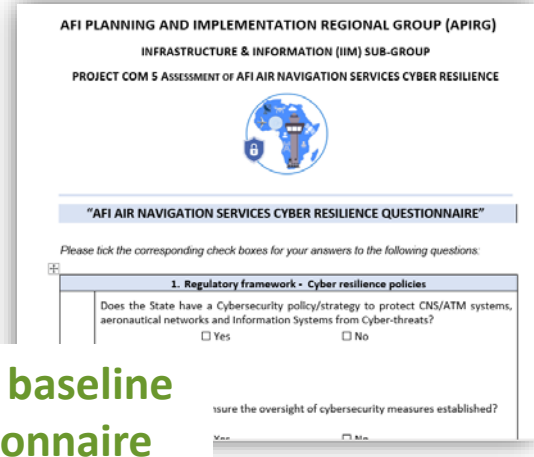
## 2.2 Actions conducted *(Key achievements)*

**List all critical systems and data used for Air Navigation Services in AFI Region**

Based on experts ' analysis, APIRG report

# ASSESS

**Project baseline questionnaire**

To assess current cyber resilience strategies put in place

**Identification of cyber threats to ANS**

Potential cyber threats, type of cyber attacks,…

AFI PLANNING AND IMPLEMENTATION REGIONAL GROUP (APIRG)

INFRASTRUCTURE & INFORMATION (IIM) SUB-GROUP

PROJECT COM 5 ASSESSMENT OF AFI AIR NAVIGATION SERVICES CYBER RESILIENCE

"AFI AIR NAVIGATION SERVICES CYBER RESILIENCE QUESTIONNAIRE"

*Please tick the corresponding check boxes for your answers to the following questions:*

| 1. Regulatory framework - Cyber resilience policies |
|---|

Does the State have a Cybersecurity policy/strategy to protect CNS/ATM systems, aeronautical networks and Information Systems from Cyber-threats?

☐ Yes    ☐ No

...nsure the oversight of cybersecurity measures established?

# 2.2 Key achievements

## AFI ANS Cyber safety resilience Framework

APIRG
INFRASTRUCTURE & INFORMATION (IIM) SUB-GROUP
COMMUNICATION PROJECT 5

**AFI Air Navigation Services Cyber Resilience Framework**

| Document information | |
|---|---|
| APIRG Sub Group | Infrastructure & Information Management APIRG Sub Group |
| Project Title | Assessment of AFI Air Navigation Services Cyber Resilience |
| Project Number | IIM SG COM N°5 |
| Project Coordinator | Côte d'Ivoire |
| Deliverable Name | AFI Air Navigation Services Cyber Resilience Framework |
| Deliverable ID | D07 |
| Edition | 00.00.04 |
| Task contributors | |
| ASECNA, Benin, Côte d'Ivoire, Gambia, Ghana, IATA, Kenya, Nigeria, South Africa, Somalia | |

Provides **guidelines** that **AFI states and organizations can adopt to assess the cybersecurity risks, threats and vulnerability to the ANS systems and operations, methods of risk mitigating** , on a voluntary basis.

Identifies the main cyber threats and lists AFI ANS Critical systems.
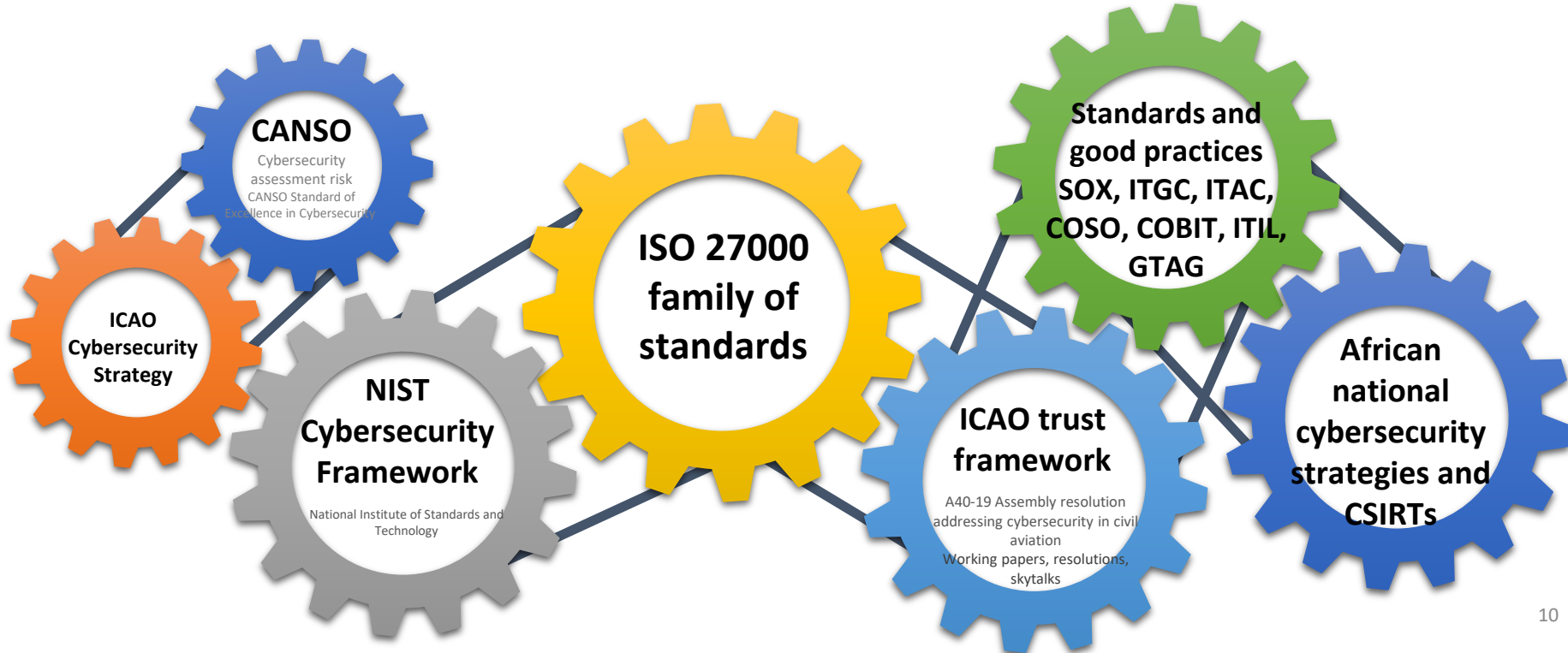
Provides a **high-level guidelines and practices on cyber resilience rather than detailed technical specifications**

## 2.2 Key achievements

… based on proven cybersecurity standards, frameworks and existing guidelines

ICAO Cybersecurity Strategy

CANSO
Cybersecurity assessment risk CANSO Standard of Excellence in Cybersecurity

NIST Cybersecurity Framework
National Institute of Standards and Technology

ISO 27000 family of standards

Standards and good practices SOX, ITGC, ITAC, COSO, COBIT, ITIL, GTAG

ICAO trust framework
A40-19 Assembly resolution addressing cybersecurity in civil aviation
Working papers, resolutions, skytalks

African national cybersecurity strategies and CSIRTs

## 2.2 Key achievements

# AFI ANS Cyber safety resilience Framework

Status

| TABLE OF CONTENT | Status |
|---|---|
| CHAPTER 1 : INTRODUCTION | ✓ |
| CHAPTER 2: UNDERSTANDING CYBER THREATS IN CIVIL AVIATION | ✓ |
| CHAPTER 3: ASSET MANAGEMENT | ✓ |
| CHAPTER 4: RISK ASSESSMENT AND MANAGEMENT | ✓ |
| CHAPTER 5: TRAINING AND AWARENESS MEASURES | ✓ |
| CHAPTER 6: DETECTION | ✓ |
| CHAPTER 7: RESPONSE | ✓ |
| CHAPTER 8: RECOVERY | ✓ |
| CHAPTER 9 : CONCLUSION AND RECOMMENDATIONS | ✓ |

RECOVER

IDENTIFY

RESPOND

PROTECT

DETECT

## 2.2 Key achievements



**Injection of false information in CPDLC**

**Surveillance Data spoofing / corruption**

**Malware injection during CNS/ATM maintenance**

**Login usurpation on ATC system technical position**

**Spoofing of GPS time**

**Spoofing of ADS-B radio signal**

**Denial of Service attack on Aeronautical Information servers**

**Software manipulation or third-party API/software**

CPDLC

Airport ATC
proach ATC
Enroute ATC
MET
AIS
AOC
Surveillance infrastructure
Navigation infrastructure
Suppliers

**Air Navigation Services - Cyber-threats landscape**
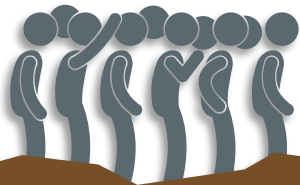*(Examples §section 2.5 of ANS Cyber resilience Framework)*

# 2.3 Challenges

Risks

1) Project baseline questionnaire and States response
2) Experts's availability and validity
3) Keeping the framework up-to-date with developments in this area until final approval by APIRG

## Project Current status

1. The project baseline questionnaire on ANS Cyber resilience had been finalized since mid 2018 but not yet sent to AFI States
2. Low level of participation of experts
3. A consolidated version of the framework finalized in January 2020

## Project Goals

1. Current state of ANS cyber safety resilience in AFI region
2. Experts involved in the project (cooperation with other regional initiatives)
3. A final edition of the cyber framework up-to-date and in line with ICAO latest developments

# 2.4 The Way Forward

*Project Upcoming Tasks and Milestones*

**Organize a webinar to raise cyber safety and resilience awareness for ANS**

*Resp. IIM COM 5, IIM Chair*

**Keep up-to-date the AFI ANS Cyber safety and resilience**

With :
- latest input/information from ICAO Working Group on Air Navigation Systems (WG-ANS) of the ICAO SSGC,
- Survey conducted through the project questionnaire **(March 2021)**

**Close out of the project**

*(Phase 1)*

*To be validated with IIM SG chair/ Secretariat*

**Nov 20** — **Nov/Dec 2020** — **Feb. 2021** — **April 2021** — **May – Sept 2021** — **Dec. 2021**

**Project baseline questionnaire survey to be sent by IIM Secretariat**

Online meeting with all IIM projects
Involvement of other regional initiatives (EU, )

**Review by IIM SG of the proposed AFI ANS Cyber safety framework**

Resp. IIM Chair and Secretariat

**Webinars/workshop/informati on sessions to raise awareness on the framework**

Resp. IIIM COM 5, IM Chair and Secretariat

# 3. Action by the Meeting

**3.1 The meeting is invited to:**

a) Take note of the progress of the project.

b) Note the difficulties encountered by the project and identify any possible solutions with other IIM projects.

c) Encourage cooperation with other regional initiatives on ANS Cyber safety and resilience *(e.g. SAT working group on ANS cybersecurity, EATM CERT, …)*

d) Urge States to participate actively in the project and in future Cyber Security and Resilience awareness workshops/webinars.
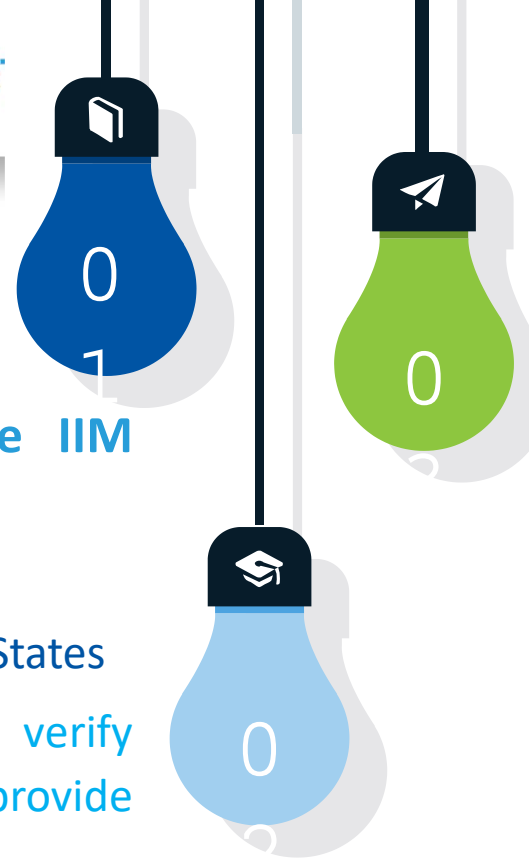
# 3. Action by the Meeting

**3.2 Draft Conclusion/Decision : Effective support to the IIM Projects activities**

That;

1) Secretariat to send the project baseline questionnaire to AFI States

2) States to confirm the list of project members and verify availability/validity of their designated experts and to provide feedbacks on the project questionnaire

3) APIRG to support activities to raise awareness of ANS Cyber safety and resilience (*through webinars/workshops/seminars on Cyber safety and resilience for AFI Region*).

16