



# AFI PLANNING AND IMPLEMENTATION REGIONAL GROUP (APIRG)

INFRASTRUCTURE AND INFORMATION MANAGEMENT SUB GROUP

COMMUNICATION PROJECT N°5



## « ASSESSMENT OF AFI AIR NAVIGATION SERVICES CYBER RESILIENCE »

Sandrine Gnassou, project coordinator,  
Head of CNS Department , Côte d'Ivoire CAA

# PRESENTATION OBJECTIVES

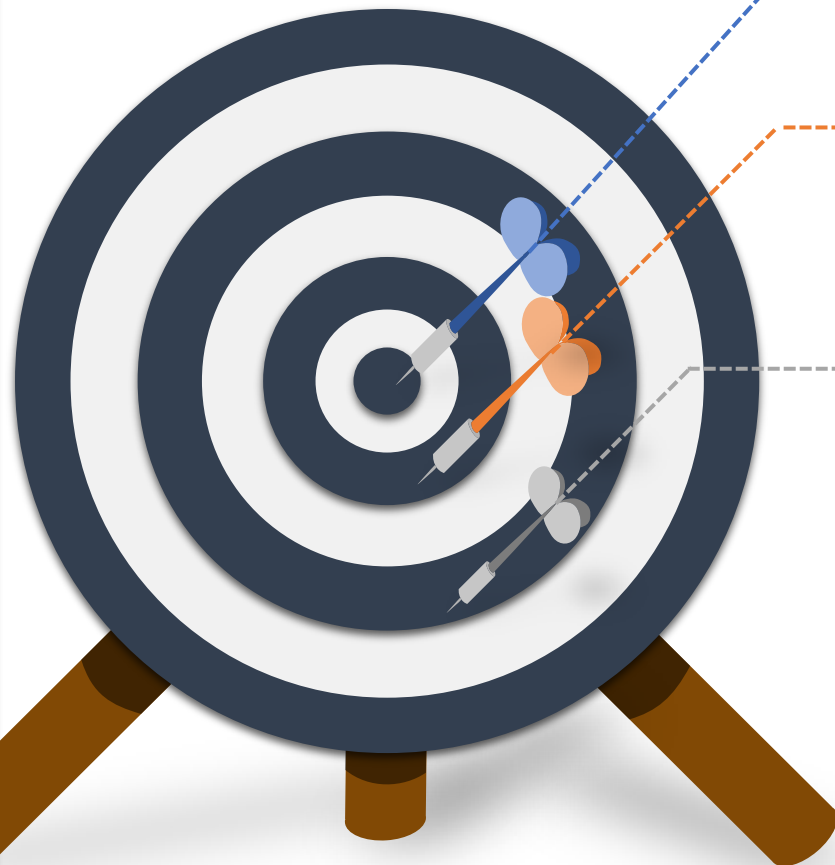


Provide an overview of an ongoing initiative on Air Navigation Services Cyber safety and resilience in Africa

*APIRG IIM COM 5 project key achievements and the challenges*

Propose some recommendations on future steps concerning ANS Cyber resilience at a regional level

Raise awareness about cyber threats to Air Navigation Services in Africa



# AGENDA

**1. INTRODUCTION**

**2. APIRG IIM SUB GROUP COM 5 PROJECT DESCRIPTION**

**3. PROJECT STATUS : KEY ACHIEVEMENTS AND NEXT STEPS**

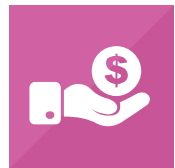
**4. CONCLUSION**



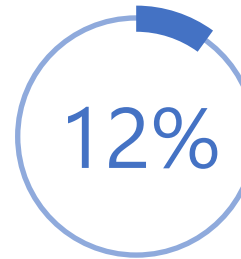
# INTRODUCTION



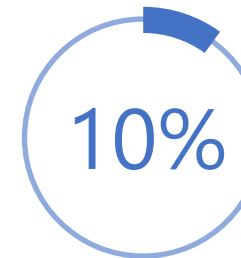
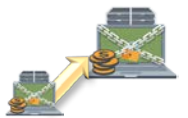
### Cyber attacks are increasing and evolving...



Cyber-crime damages will cost the **world \$6 trillion** annually by 2021\*

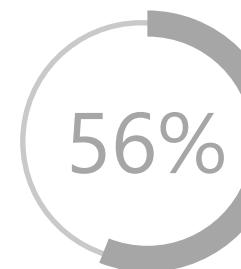


increase in enterprise ransomware



Malicious URLs

One in ten URLs are malicious



WEB Attacks

Increase by 56%



“There is a hacker attack on computers with Internet access, on average every 39 seconds (in US)”\*\*\*

Sources : (\*) 2017 Cybersecurity Ventures, Symantec's 2019 Internet Security Threat Report (ISTR),

<https://www.everycloud.com/cyber-security-facts>

(\*\*) <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>

(\*\*\*) <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>

# INTRODUCTION

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



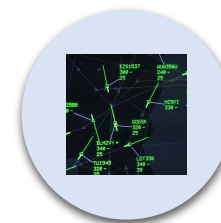
AIRPORT



AIRCRAFT



AIRLINES



AIR TRAFFIC  
MANAGEMENT

# INTRODUCTION

Aviation Cyber-attack surface is growing...



Increasing Connectivity and use of non-protected by design A/G Data Link Communication

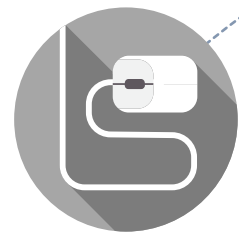
Increased use of commercially available information technology (COTS)

Migration for interoperability to standard IP-based network

with publicly available vulnerabilities

More interconnected systems and information sharing

Less isolated architectures  
More Network centric infrastructure and operations





# INTRODUCTION

## International efforts



**Resolution A39-19 Addressing Cybersecurity in Civil Aviation ...** calls States and Industry to identify threats and risks, understanding and coordination, promote standards and best practices, promote cybersecurity culture ..(..)

**December 2014**

Civil Aviation  
Cybersecurity Action Plan

**April 2017**

Dubai Declaration on  
Cyber Security in Civil  
Aviation

**December 2017**

Global Air Navigation  
Industry Symposium  
(GANIS) 2017

**July 2018**

2nd Meeting of the  
APIRG Information and  
Infrastructure  
Management Sub-Group  
(IIM/SG2)

**October 2019**

Aviation Cybersecurity  
Strategy

ICAO A39 -19  
Cybersecurity Resolution

**October 2016**

1st meeting of APIRG IIM  
Sub group

*Launch of IIM COM 5 project  
"Assessment of AFI  
aeronautical networks  
cybersecurity"*

**August 2017**

Summit on Cyber Security  
in Civil Aviation Europe,  
Middle East and Africa  
(EMEA) - Bucharest,  
Romania

**May 2018**

13th Air Navigation  
Conference  
(Recommendation 5.4/1 –  
Cyber resilience)

**October 2018**





# AN AFI REGIONAL INITIATIVE

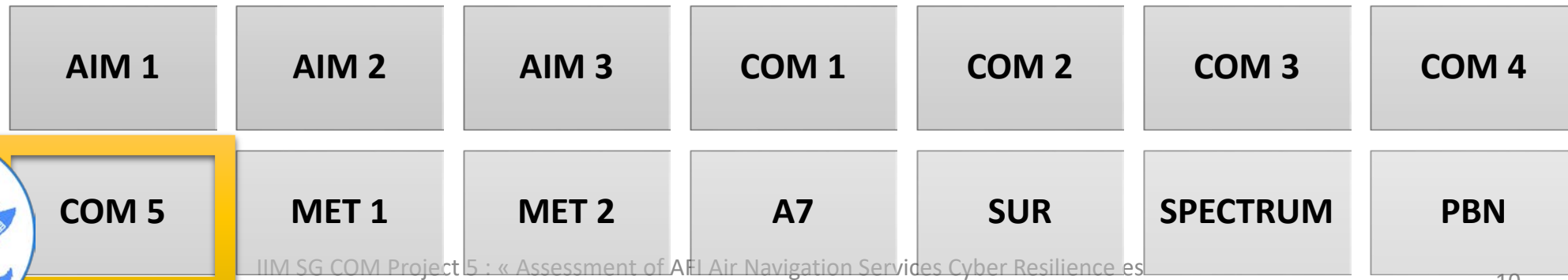
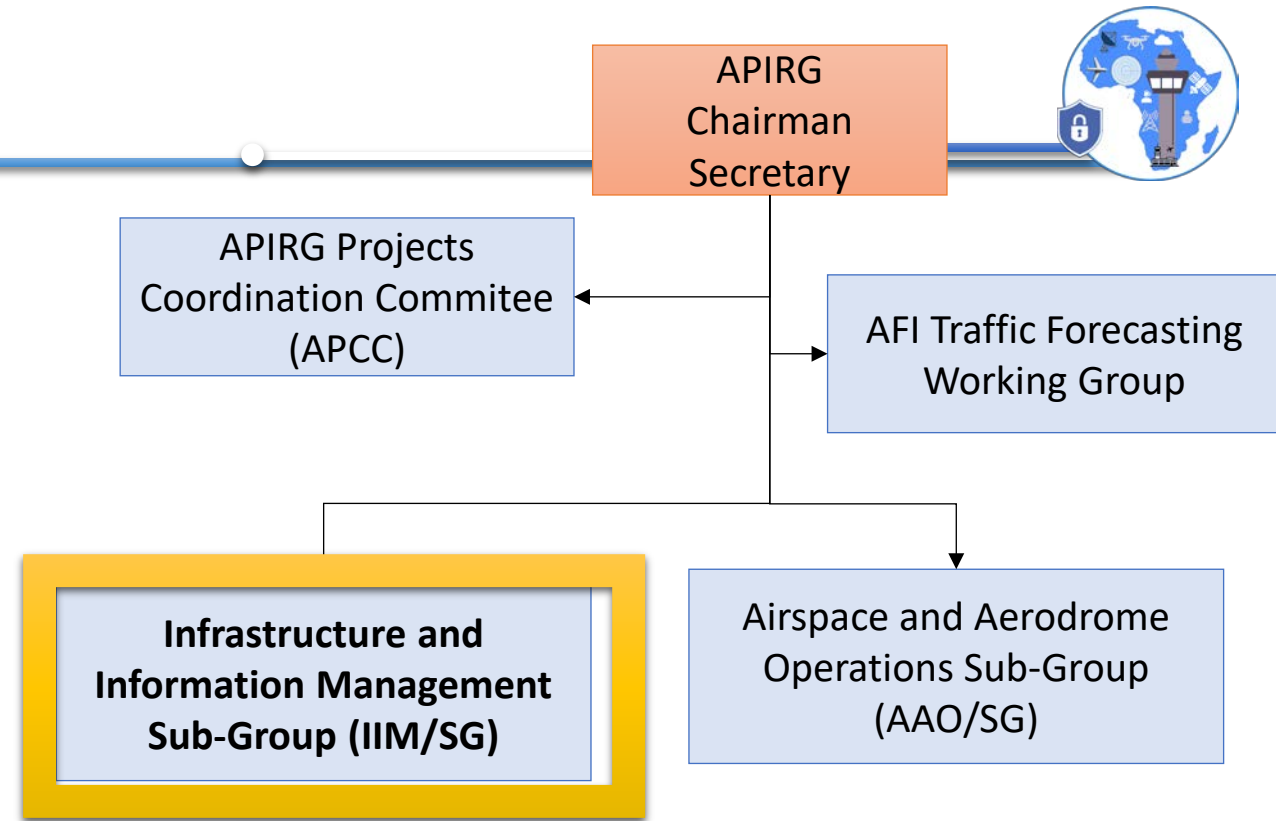
IIM SG COM Project 5

« *Assessment of AFI Air Navigation Services Cyber Resilience* »



# PROJECT DESCRIPTION

- A project of APIRG Infrastructure and Information Management (IIM) sub-group project
- Communication Project N°5 : « **Assessment of AFI Air Navigation Services Cyber Resilience** »
- Project coordinator : Côte d'Ivoire CAA



# PROJECT DESCRIPTION



## 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 resilience framework for Air Navigation Services

## Project Members

*AIS, CNS experts, Cybersecurity and IT experts, ANS Safety oversight inspectors from :*



Benin



Kenya



Côte d'Ivoire



Nigeria



Gambia



Somalia



Ghana

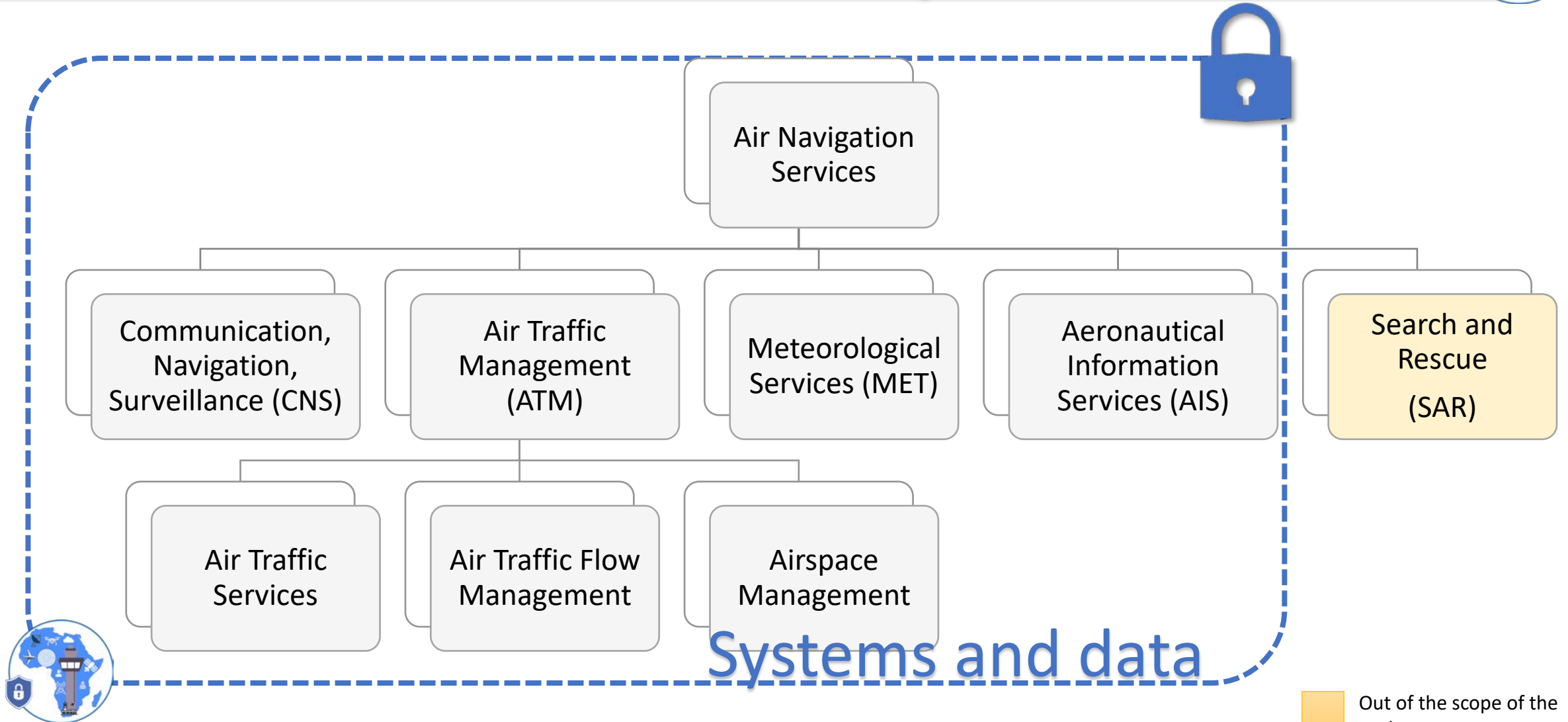



South Africa



# PROJECT DESCRIPTION

Project Scope



 Out of the scope of the project

# PROJECT DESCRIPTION

## Project Scope



### 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



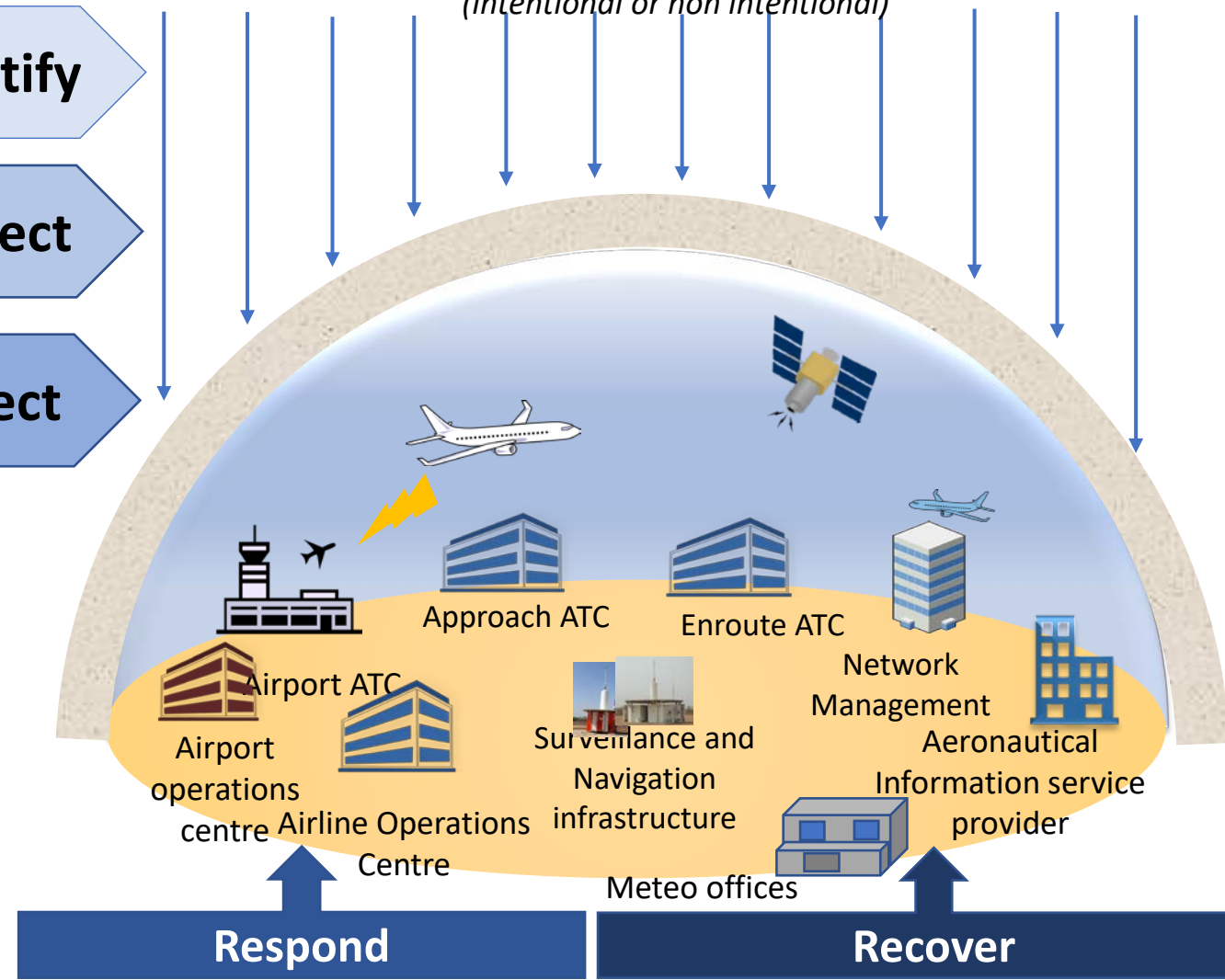
Identify

Protect

Detect

Cyber threats

(intentional or non intentional)



# PROJECT DESCRIPTION

## Project Phases



### Project Definition



### ANS cyber risk assessment





### Regulatory analysis







### AFI ANS Cyber resilience framework





### 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 
- cyber threats to ANS 

Analysis of existing cybersecurity and cyber resilience frameworks and guidelines (ISO 27000 series, NIST framework, ICAO thrust framework) 

Development by the project team (project internal validation) 




Review by IIM and Secretariat 

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

# PROJECT DESCRIPTION

## Project main tasks

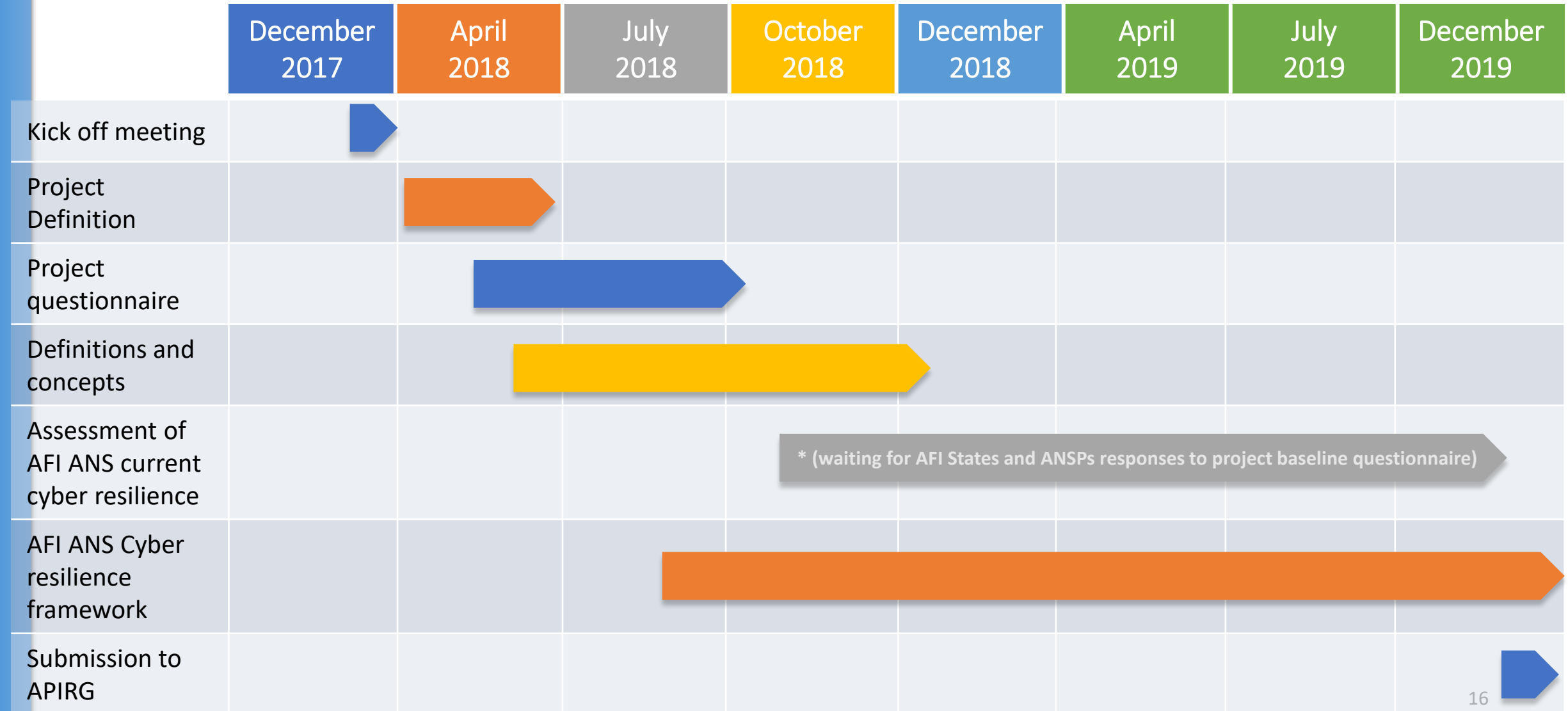


	Key activities	Main Tasks
<b>PROJECT DESCRIPTION</b>	<p><b>Project description and scope</b></p>	<ul style="list-style-type: none"> <li>• Define the project Scope</li> <li>• Agree on Project Terms of Reference</li> <li>• Develop and keep up to date the Project Description, organization and linkages with other IIM Projects</li> </ul> 
<b>CYBER THREATS ASSESSMENT</b>	<p><b>Assessment of cyber resilience of Air Navigation services in Africa</b></p>	<ul style="list-style-type: none"> <li>• List all systems and data used for Air Navigation Services in AFI Region (expert knowledge , APIRG reports,...)</li> <li>• Develop Project baseline questionnaire and analyze AFI States and ANSPs feedbacks (through questionnaire)</li> <li>• Identify the main cyber threats (ENISA reports, Symantec, Aviation cyber incidents information )</li> </ul>
<b>CYBER FRAMEWORK</b>	<p><b>Development of an AFI ANS Cyber resilience Framework</b></p> 	<ul style="list-style-type: none"> <li>• Analyze existing cybersecurity and cyber resilience frameworks (ISO 27000 series, NIST framework, ICAO thrust framework)</li> <li>• Develop an AFI Cyber resilience framework for Air Navigation services</li> </ul> 



# PROJECT DESCRIPTION

## Project timeline





# KEY ACHIEVEMENTS

# KEY ACHIEVEMENTS



### 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

Comments (if any)

01

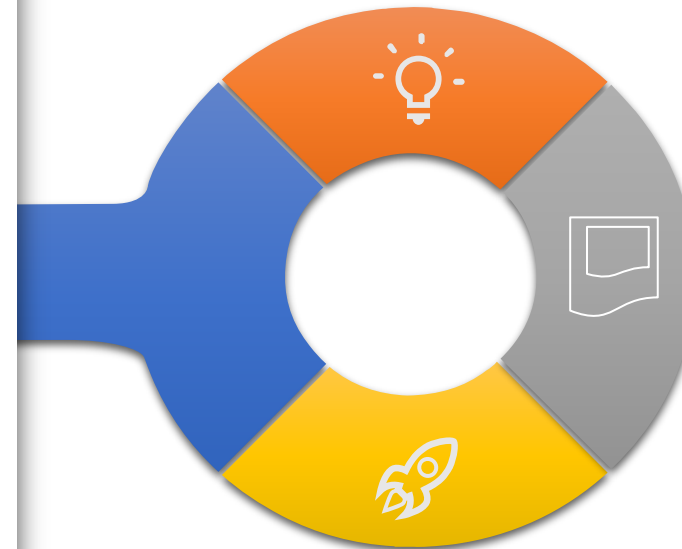
If Yes, does the State ensure the oversight of cybersecurity measures established?

Yes

No

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

Based on experts ' analysis, APIRG reports,...



### Identification of cyber threats to ANS

Potential cyber threats, type of cyber attacks, ...

### Project baseline questionnaire

To assess current cyber resilience strategies put in place

# KEY ACHIEVEMENTS

## AFI ANS Cyber resilience Framework



The proposed AFI Air Navigation Services Cyber resilience Framework :



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

### AFI Air Navigation Services Cyber Resilience Framework

#### Document information

APIRG <a href="#">Sub Group</a>	Infrastructure & Information Management APIRG <a href="#">Sub Group</a>
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

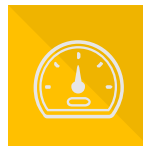
ASECNA, Benin, Côte d'Ivoire, Gambia, Ghana, IATA, Kenya, Nigeria, South Africa, Somalia



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.

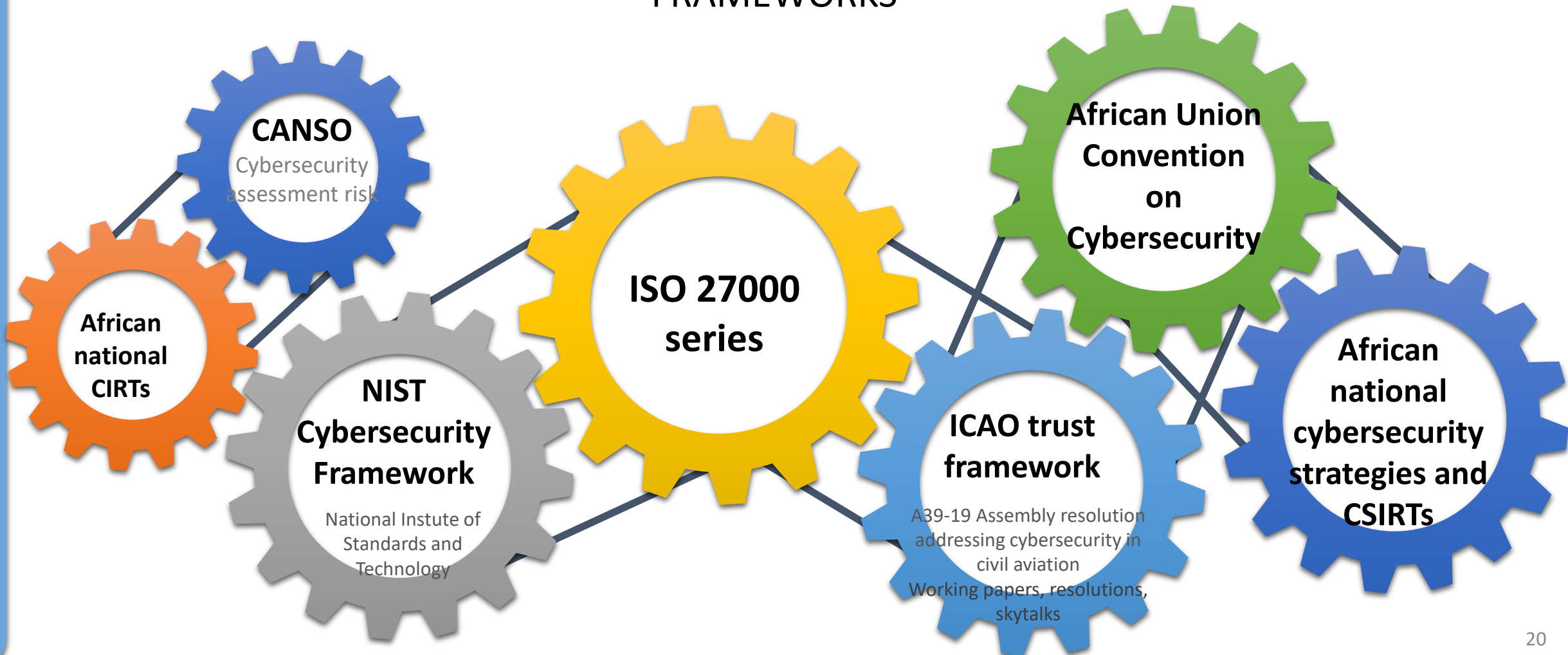


Provides a **high-level guidelines and practices on cyber resilience rather than detailed technical specifications** and are **based on proven cybersecurity standards and frameworks (ISO 27000 series, NIST)**

# KEY ACHIEVEMENTS



WE ARE BUILDING ON EXISTING INITIATIVES AND CYBER SECURITY FRAMEWORKS



# KEY ACHIEVEMENTS

How can ANS be resilient to cyber threat?



Business continuity plans to maintain resilience and recover capabilities after a cyber breach



Identify primary assets (« crown jewels »)  
Risk Management  
Develop formal Cyber Policies

Threat Intelligence  
contingency planning, procedures, and training and awareness

Protect assets according to risk  
Build Cybersecurity culture : training, education, awareness  
Build layered system

Cyber monitoring  
Networking to share cyber info, to predict new threats and be prepared

Source : NIST (National Institute of Standards and Technology) Framework

# KEY ACHIEVEMENTS

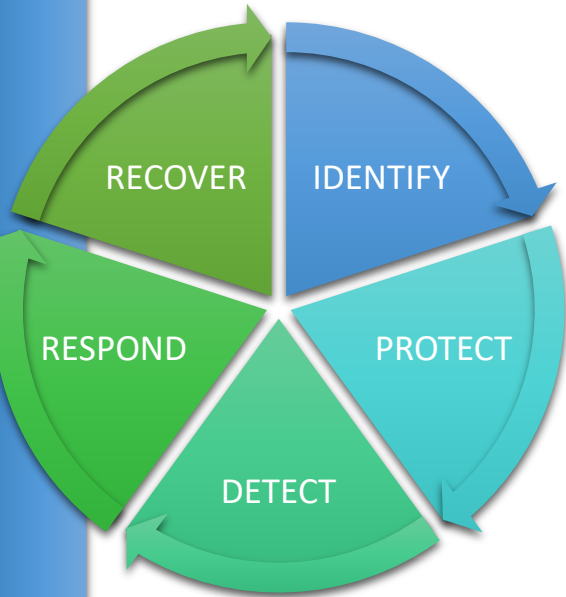
## AFI ANS CYBER RESILIENCE FRAMEWORK



Status

### TABLE OF CONTENT

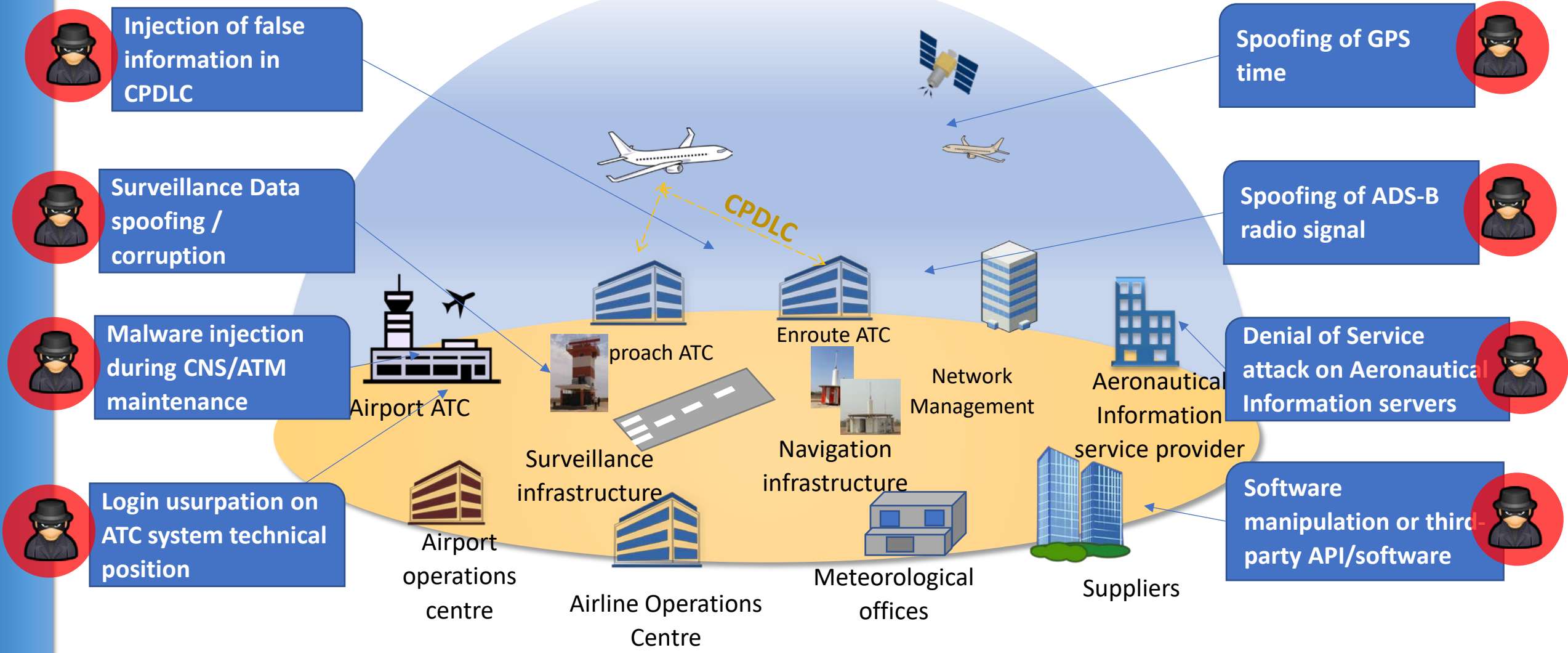
CHAPTER 1 : INTRODUCTION	✓
CHAPTER 2: UNDERSTANDING CYBER THREATS IN CIVIL AVIATION	✓
CHAPTER 3: ASSET MANAGEMENT	✓
CHAPTER 4: RISK ASSESSMENT AND MANAGEMENT	✓
CHAPTER 5: TRAINING AND AWARENESS MEASURES	✓
CHAPTER 6: DETECTION	✓
CHAPTER 7: RESPONSE	✓
CHAPTER 8: RECOVERY	✓
CHAPTER 9 : REGULATORY AND STANDARD COMPLIANCE REQUIREMENTS	✗





# KEY ACHIEVEMENTS

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



# KEY ACHIEVEMENTS

Project coordination



## Objective Focus

Agreed project organization and a robust coordination mechanism which enabled the development of a mature version of a proposed AFI ANS Cyber resilience framework



## Expertise

Engagement and involvement of IT, CNS and AIS senior Experts (key actors)



## Teamwork

More than 25 online meetings / Teleconferences scheduled and coordination by emails

“ Successful South – South Cooperation “



# CONCLUSION

# CONCLUSION



01



Need to support the creation of a cyber resilience framework AFRICA needs

*We need to work together , and develop a framework in line with ICAO thrust framework and other regional cyber frameworks (European, ..)*

02



Establish close coordination with other IIM projects (AIM, MET, SURV, SPECTRUM) to ensure that all aspects of cyber resilience (identified in these projects) are included in the IIM COM project deliverables

03



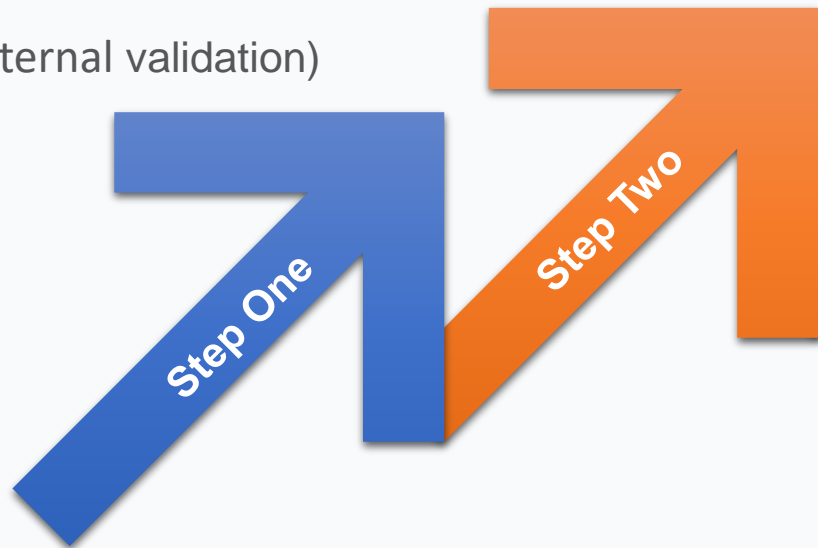
The project baseline questionnaire on ANS Cyber resilience should be sent to AFI States and Organizations to have the current state of ANS cyber resilience in AFI region

# CONCLUSION



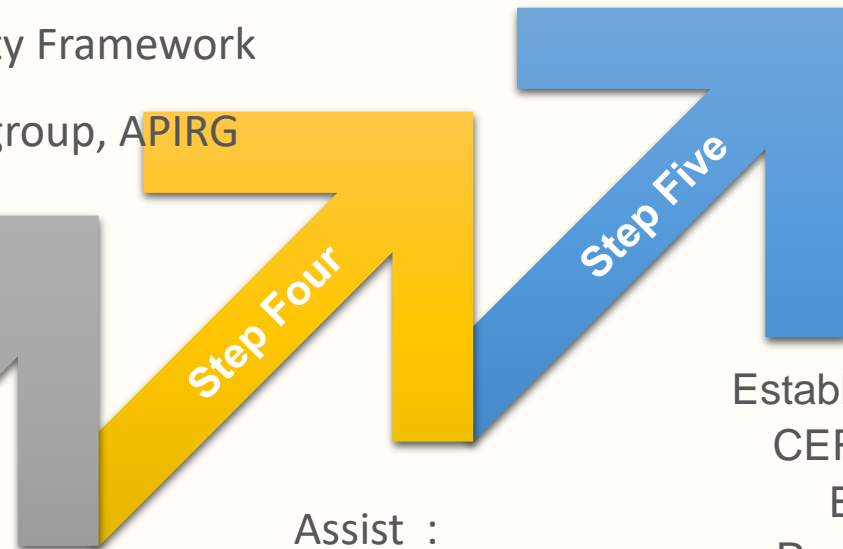
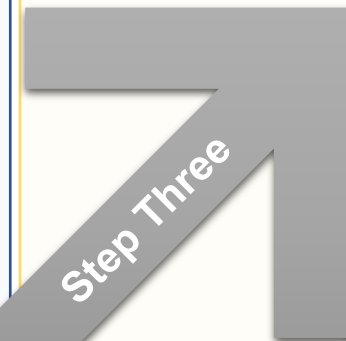
## IIM COM 5 Project Scope

Validation of the AFI ANS  
Cybersecurity Framework  
Finalization of the AFI ANS by IIM Subgroup, APIRG  
Cyber resilience Framework  
(Project internal validation)



## Out of the project scope – potential next steps

Validation of the AFI ANS  
Cybersecurity Framework  
by IIM Subgroup, APIRG



Assist :

- (1) the member organizations establish and develop a CSIRT (Computer Security Incident Response Teams) **(internal to the ANSP/organization)**
- (2) the member organizations CSIRT s to implement their cybersecurity policies, plans and procedures

Establish **AFI Region**  
CERT (Computer  
Emergency  
Response Team)  
(e.g. AFI Centre for  
Cybersecurity in  
Aviation)



THANK YOU