SOUTH AFRICAN
CIVIL AVIATION AUTHORITY
Keeping you safe in the sky

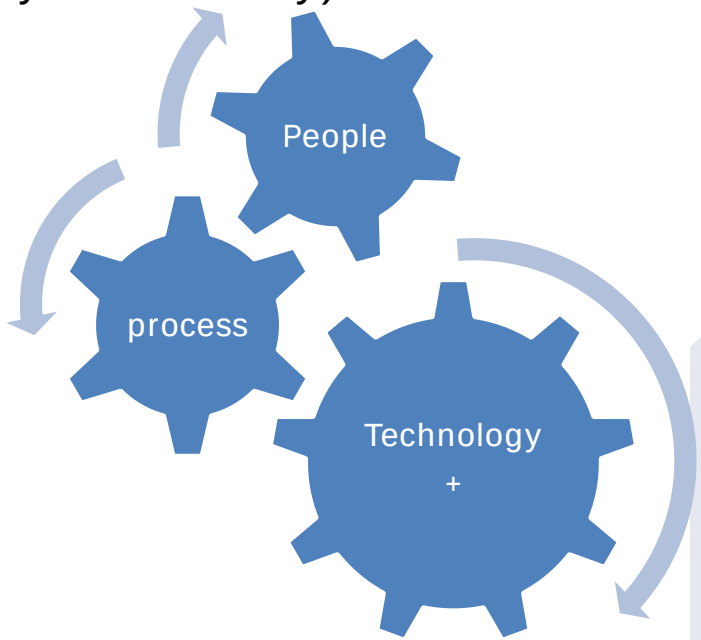
RSA –AVSEC Cybersecurity Approach

Presented by: Dikeledi Mzimba

South African Aviation Proactive approach

The South African Civil Aviation Authority(SACAA) in response to addressing the cybersecurity and safeguarding against unlawful during the financial period 2020/2021 an industry cybersecurity strategy was approved .

- Formulated under Aviation Security recognizing the imminent risk –cybersecurity
- Acknowledge the cross- cutting nature of cybersecurity (safety and security)
- Competent resource to respond to cyber need (recruitment)
- Develop a cybersecurity culture and awareness



South African Aviation Proactive approach

Why the strategy approach

Considering that the Authority oversight mechanism had not ventured into addressing information security principle nor cybersecurity .

The developments of the strategy served to:

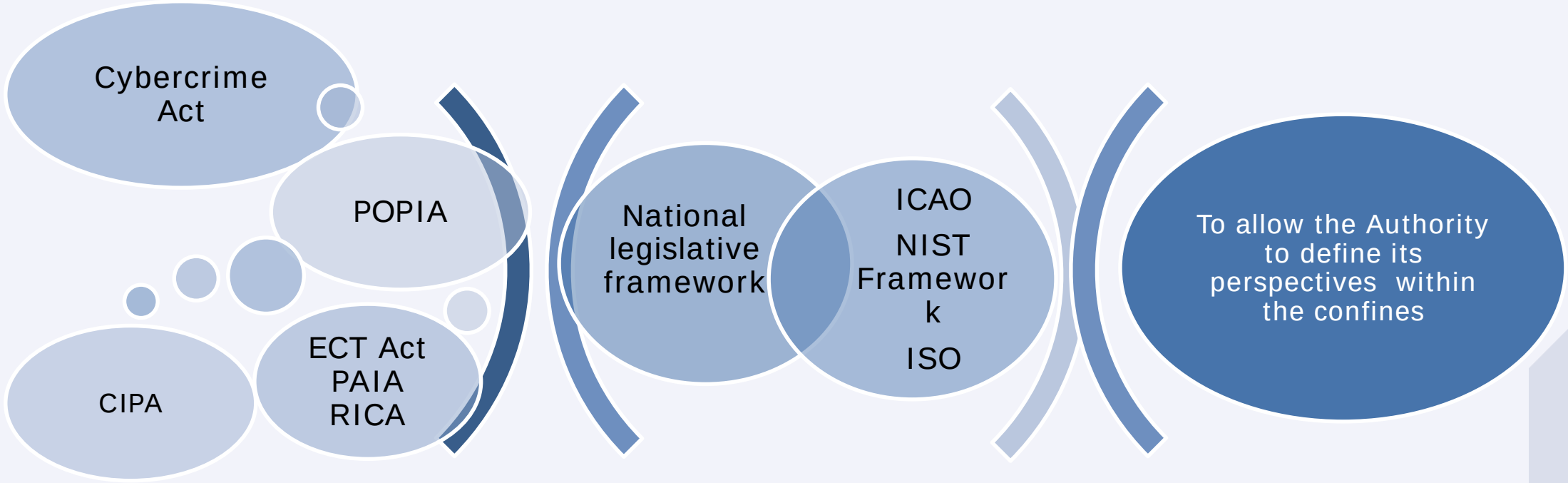
- Provides a proactive approach rather than reactive
- Define the authority cyber perspective
- Engaged National cybersecurity legislation
- Unpack the National cyber landscape

Why not the review of the NASP?

- Involved prolonged process …
- Regulatory amended feasible –Annex 17 chapt 18

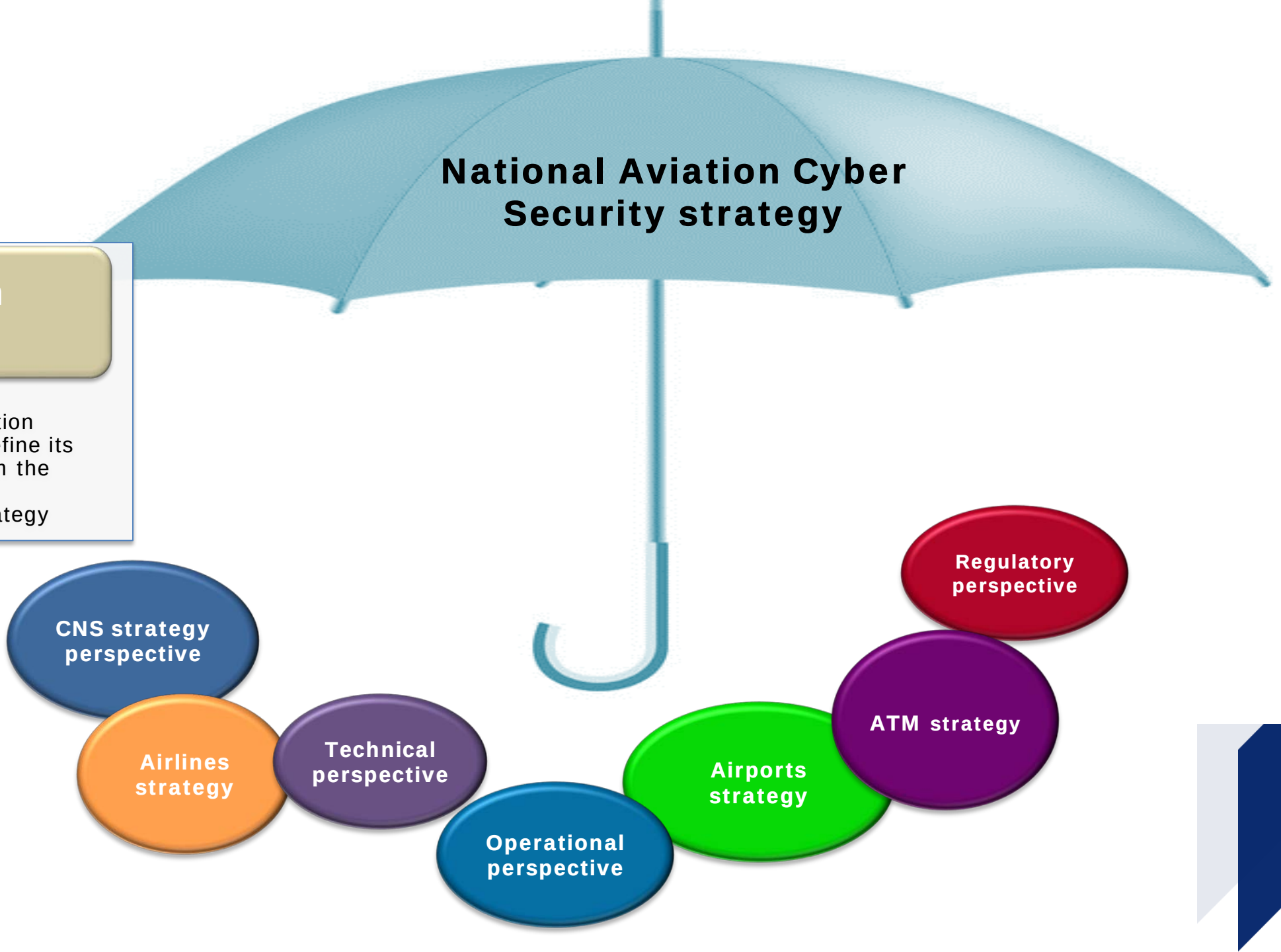
Drivers of Aviation Cybersecurity

This was informed the National Cybersecurity Policy framework (NCPF) of 2013 and other legislative framework to inform the information security which identified role players involved to facilitate , coordinate and a manage cybersecurity within the country .



Defining aviation perspective

•Each entity within the aviation ecosystem responsible to define its perspective which will inform the overarching holistic and comprehensive National strategy



Industry strategy process

The management of cybersecurity issues requires an ***integrated proactive approach*** to identify and mitigate the cyber threats targeted towards aviation's to provide a baseline to guide the Authority.

A systematic *five phase strategy developments* process was adopted. This was evident in the *needs* and *gaps* analysis conducted, to provide understanding and perspective of our own cyber risks.

A prolific opportunity to share and identify relevant information and understanding of the aviation entities involved

It was imperative that the Authority engage with its industry as this was depended on a *mind shift* and *behavioural change* which only could be possible through evaluation of the organisation response to cybersecurity and its culture

Authority -Current Efforts

Step 1: Adoption of the ICAO Cybersecurity Strategy

Step 2: Development of the Industry Cybersecurity strategy for the protection of civil aviation infrastructure systems and data against cyber-attacks. Through consulting the necessary guiding principles, regulatory prescripts and best practices for a comprehensive approach .

Step 3: Amendments of SACAA regulatory prescript to incorporate measures to mitigate aviation cyber risk and threats and to maintain CIA through the adoption of best practice to achieve security and resiliency

Step 4: Development of Action plans mapped with the ICAO Action plan to achieve harmonisation . To ensure resource allocation, capacity and culture is created to adequately response to aviation cyber risk and threats .

Step 5: Adopt a risk based approach based on common understanding of threats and risk to protect critical aviation systems through the implementation of cybersecurity management system.-NIST , CIA , ISO 27000 (cyber risk matrix)

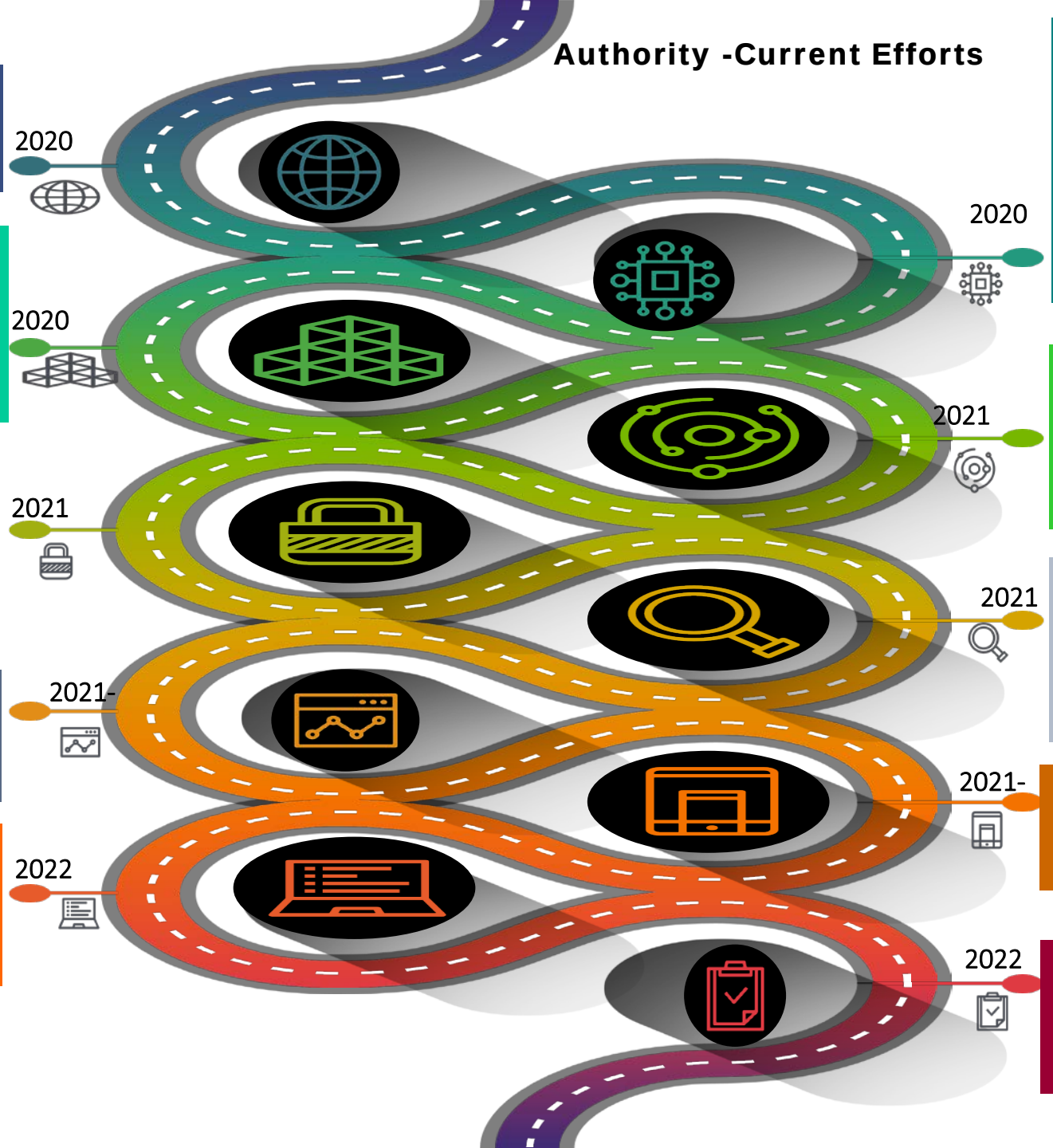
Step 6: To establish a coordinated and collaborative efforts – Cybersecurity Advisory Committee and incident management. To ensure civil aviation industry participation into cyber issues

Step 7: Creating a cybersecurity culture, partnership and sharing of information and capability exposure, risk to establish maturity.

Step 8: Ensuring that cybersecurity form part of the CNS work , since cybersecurity is central , airports , airlines , cargo

Step 9: Development of the National Cybersecurity strategy which is holistic and incorporate how the entire aviation ecosystems is to be safeguarded

Step 10: Developments of an oversight mechanism , that support and manage cyber risk and threats and implementation of the ISMS to identify, protect , prevent , response



Partnership and Collaborative efforts

GOVERNMENT

Government to provide strategic direction and policy framework to provide critical infrastructure assurance

Legislation and Policy formulation

To conduct assessment and to provide intelligence based recommendation

Develop national cyber strategies to set out policy and regulatory measures to maintain cybersecurity at an acceptable level

Provide a national aviation threat and risk picture

Provision of teams responsible for handling cyber incident and risks

Share cyber risk & threats information

Encourage cybersecurity capabilities

strengthen cybersecurity partnership

REGULATOR

Coordination and monitoring of the implementation of proven standards for Aviation security .

Develop and implement an appropriate **regulatory framework** for the aviation cyber security informed by the global and national threat exposure

Ensure alignment and adherence to ICAO cyber requirements

Develop **cybersecurity governance principles**

Encourage and enable **information sharing a**nd **collaboration** for decision making purposes

Develop a **cyber risk** based approach for the protection of critical infrastructure system and communication

Establish a security posture management context develop common **criteria** and **language**

Encourage coordination ,collaboration and information security

Aviation Cybersecurity Advisory committee

INDUSTRY

To identify its critical assets and vulnerabilities.

Assess cyber risk and threats

Improve and adopt cybersecurity security baselines

Develop a plan to manage cybersecurity incident and emergencies

To be responsive to cyber attack

Provide periodic reports providing structural statistical summary and lesson learnt

Establish an information sharing capability

Develop third party management Practices

Develop Cyber culture and awareness

Strengthen cybersecurity partnership

THANK YOU