Session 4

Effective exchange of threat and risk related information at regional and international level

Mr. José Maria Peral Pecharroman

Regional Officer Aviation Security
and Facilitation, ICAO NACC

Mr. Leonardo Boszczowski

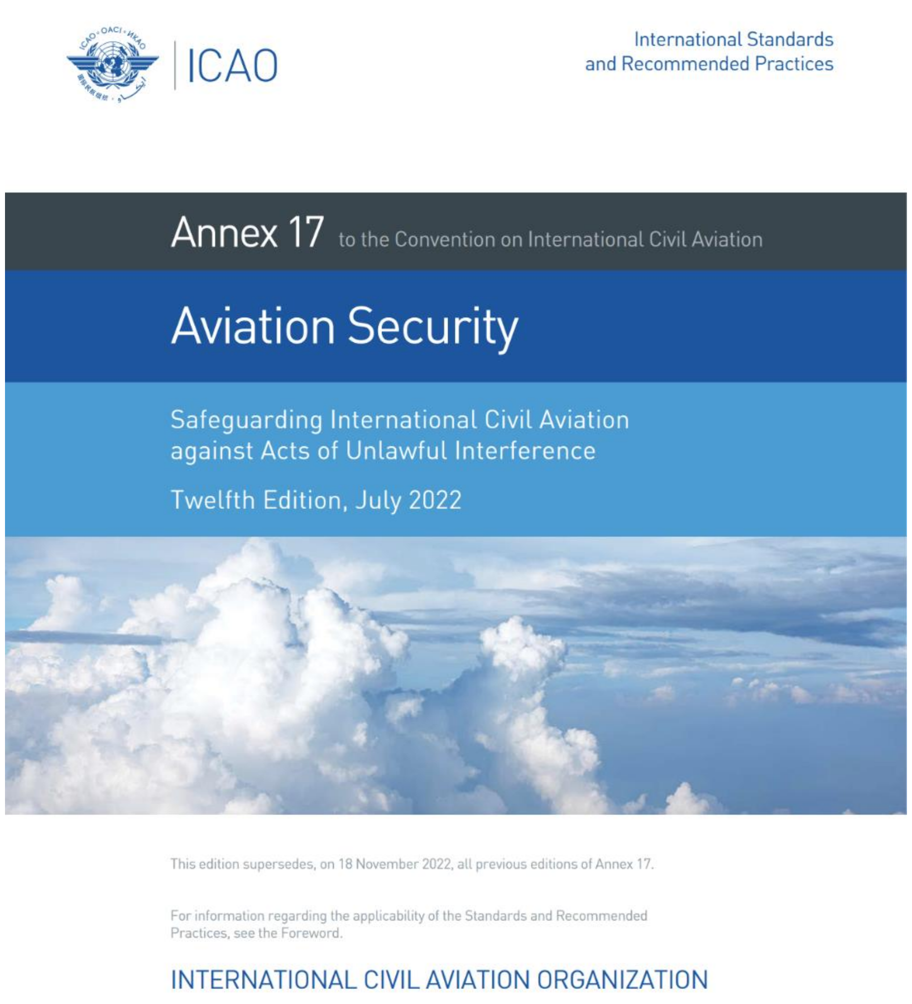
Regional Officer, Aviation Security
and Facilitation, ICAO SAM

Mr. Iván Salas

AVSEC/FAL/DG Specialist, COCESNA

Ms. Althea C Bartley

Manager Aviation Security & Facilitation,
Jamaica Civil Aviation Authority



ICAO

International Standards
and Recommended Practices

Annex 17 to the Convention on International Civil Aviation

Aviation Security

Safeguarding International Civil Aviation
against Acts of Unlawful Interference

Twelfth Edition, July 2022

This edition supersedes, on 18 November 2022, all previous editions of Annex 17.

For information regarding the applicability of the Standards and Recommended Practices, see the Foreword.

INTERNATIONAL CIVIL AVIATION ORGANIZATION

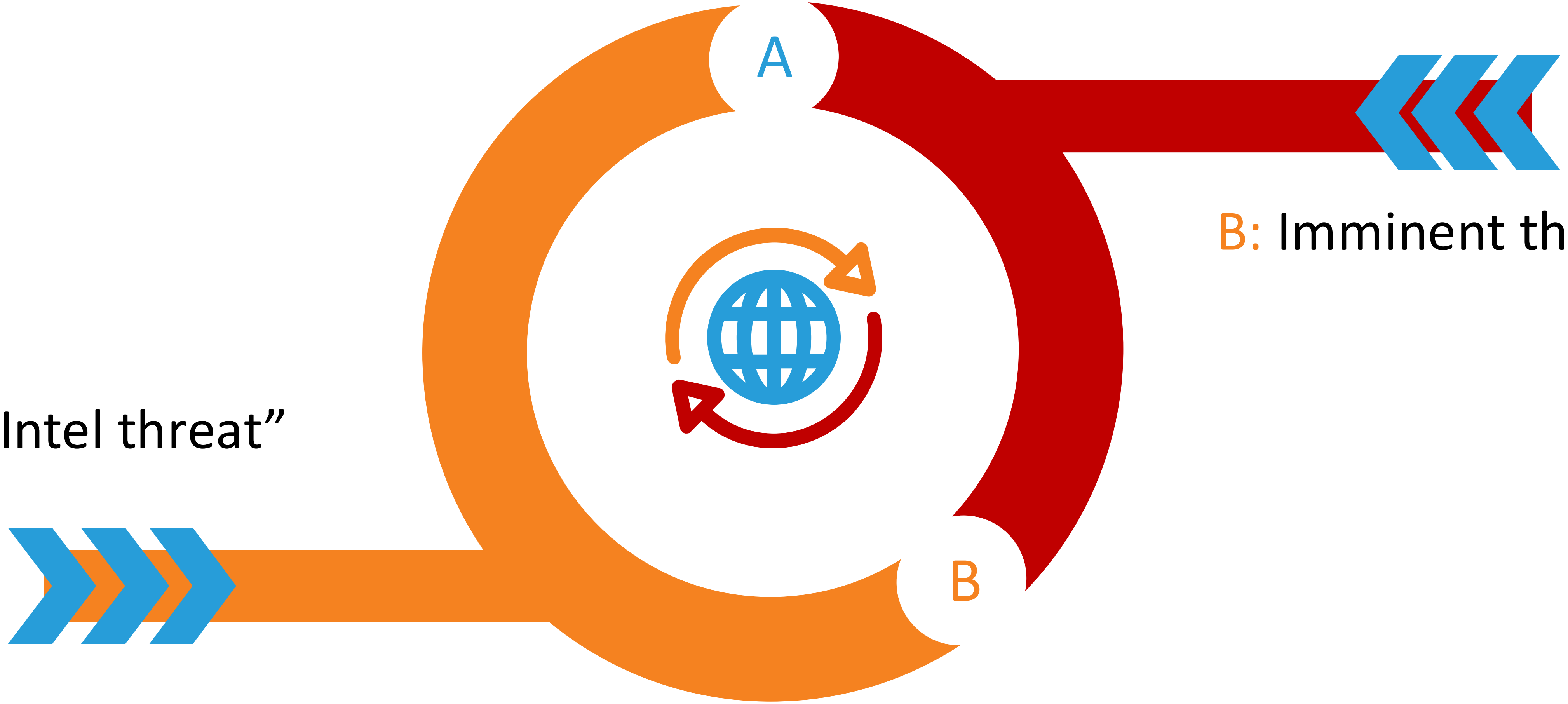
Annex 17 - Standard 2.4.4

Each Contracting State shall establish and implement procedures to share with other Contracting States, in a timely manner, threat information that applies to the aviation security interests of those States, to the extent practicable

United Nations Security Council Resolution 2309 6 (f)

Further engage in dialogue on aviation security and cooperate by sharing information, to the extent possible, about threats, risks, and vulnerabilities, by collaborating on specific measures to address them and by facilitating, on a bilateral basis, mutual assurance about the security of flights between their territories

“Types” of threat information



A:”Intel threat”

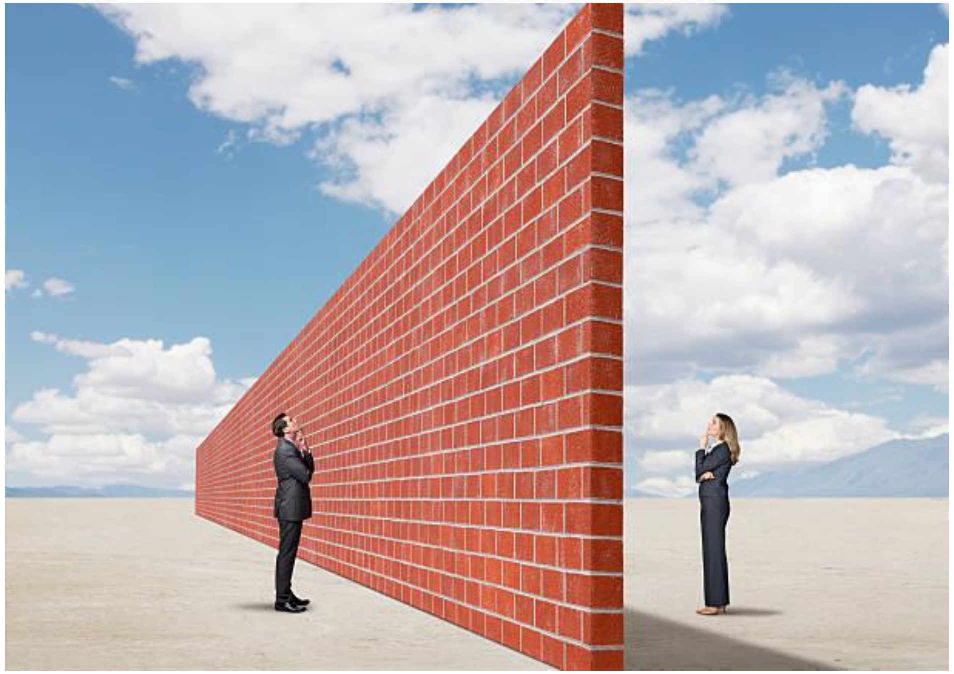
B: Imminent threat

Types of Cyber Information

- Cyber Threat Intelligence (CTI)
- Indicators of Compromise (IoCs)
- Tactics, Techniques, and Procedures (TTPs)
- Vulnerabilities
- Cyber Incident Report
- Cyber Mitigations
- Situational Awareness
- Best Practices

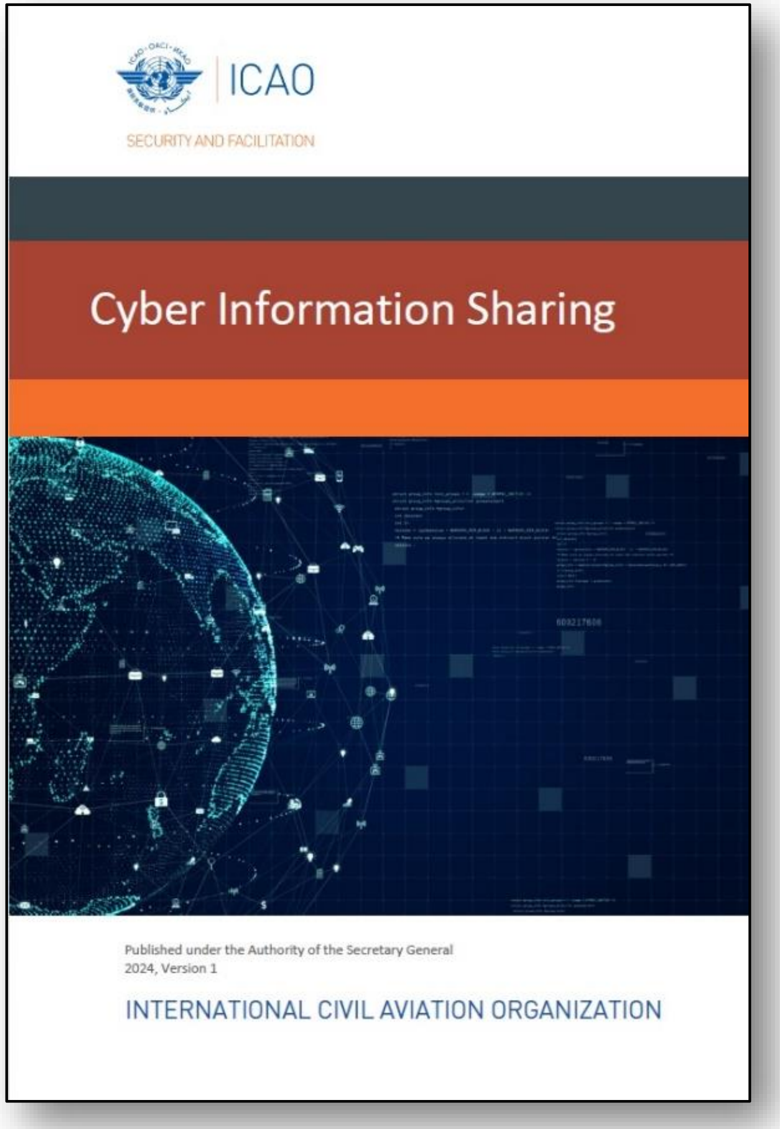
Barriers to communication and cooperation

- Lack of trust
- Lack of flexibility
- Lack of feedback
- Limited availability
- Lack of expertise knowledge
- History of friction and/or conflict
- Overlapping functions/mandates
- Purely transactional relationships
- Lack of political will and top cover
- Challenges to tech interoperability



Cyber Information Sharing

klossner
" MAYBE WE SHOULD TRY A DIFFERENT SECURITY APPROACH THIS YEAR. "


ICAO

SECURITY AND FACILITATION

Cyber Information Sharing

Published under the Authority of the Secretary General
2024, Version 1

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Cyber Information Sharing: Why is it Important?

Importance

- Provides better visibility into the cyber threat landscape to civil aviation
- Supports management of aviation cyber risks
- Promotes a collaborative approach and robust cybersecurity culture

Benefits

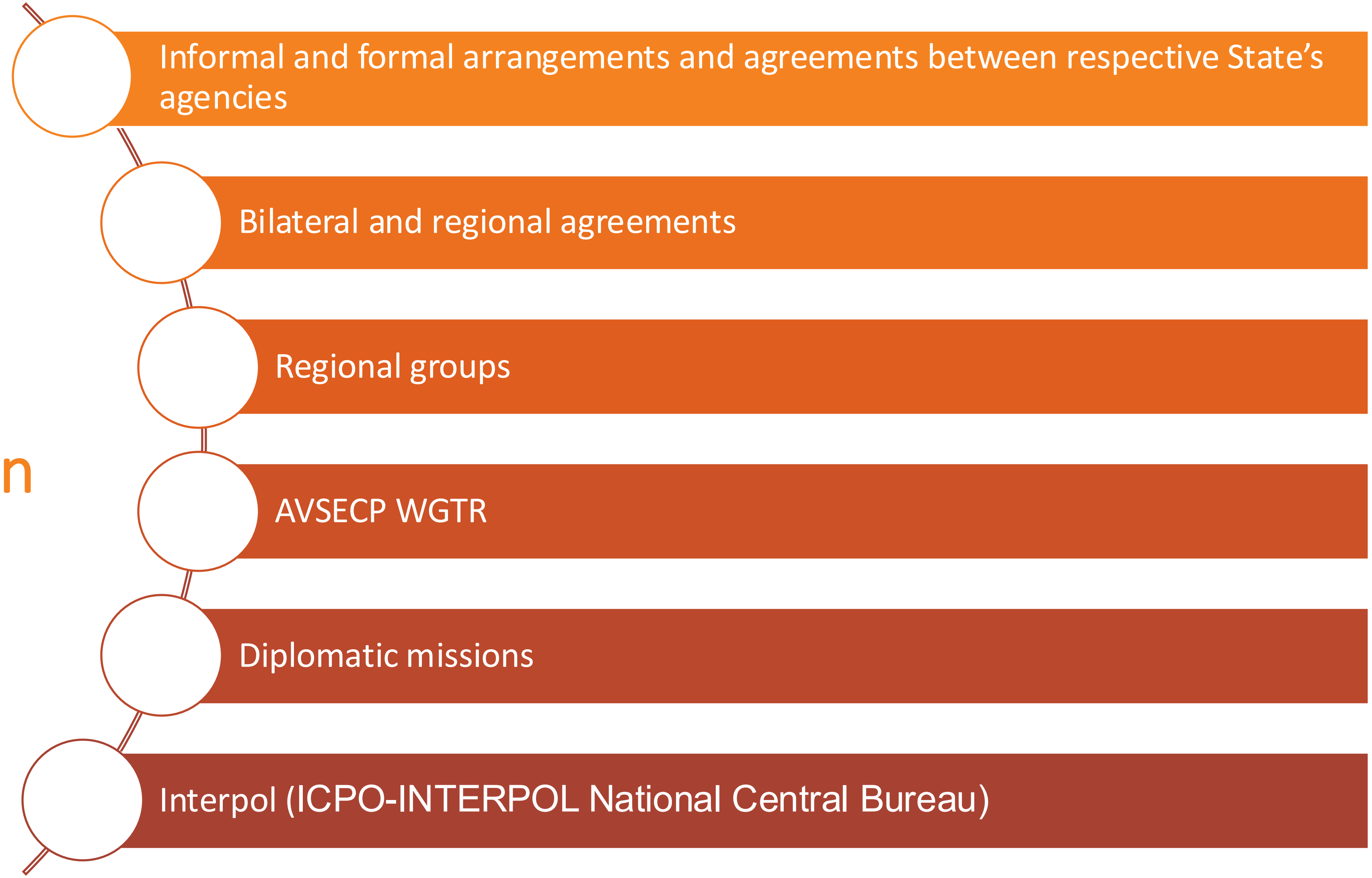
- **Strategic Planning:** Builds cybersecurity capabilities
- **Situational Awareness:** Enhances understanding of cyber threats, risks and vulnerabilities
- **Risk Management:** Improves operational and tactical management of cyber risks
- **Crisis Management:** Supports effective response to cyber incidents

Considerations

- Legal and regulatory challenges
- Resource limitations

ICAO communication channels

Examples of international communication channels



- Informal and formal arrangements and agreements between respective State’s agencies
- Bilateral and regional agreements
- Regional groups
- AVSECP WGTR
- Diplomatic missions
- Interpol (ICPO-INTERPOL National Central Bureau)

Establishment of information sharing framework

- Memoranda of understanding on information sharing, detailing principles, procedures, roles and responsibilities of all parties concerned
- the identification of a trusted group of security-cleared individuals to act as trusted communication channels, and the provision of regular threat briefings for these individuals
- promoting dialogue and interchange between national security agencies and industry
- the rapid dissemination of information about new threats or incidents to the maximum extent possible
- avoiding overly-strict use of the “need to know” principle and developing a “need to share” culture

Global Priority 1

Enhance risk awareness and response

Global Priority 2

Maintain a strong effective security culture

Global Priority 3

Develop and promote the role of human factors

Global Priority 4

Improve technological resources and foster innovation

Global Priority 5

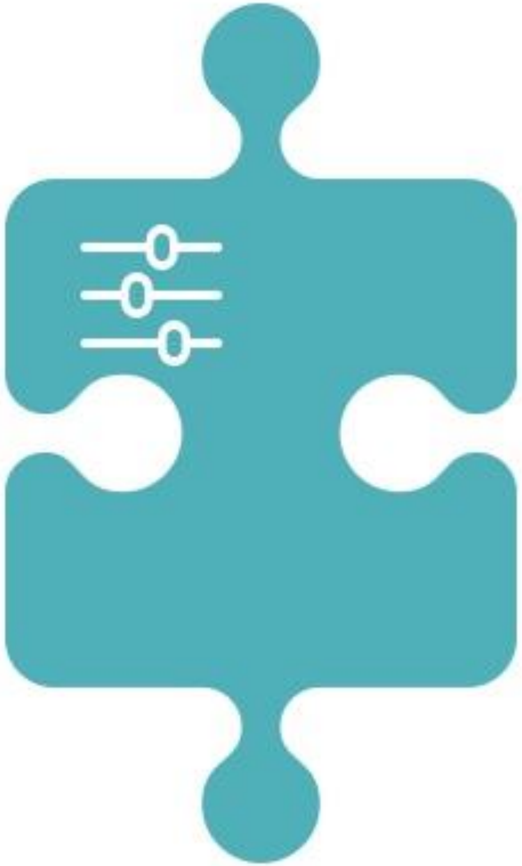
Improve oversight and quality assurance

Global Priority 6

Increase cooperation and support

Global Priority 1

Enhance risk awareness and response



- To identify, understand and manage risk, while ensuring that such efforts are targeted in the right areas, where they can have the highest impact and that emerging risks are anticipated

ICAO resources*:

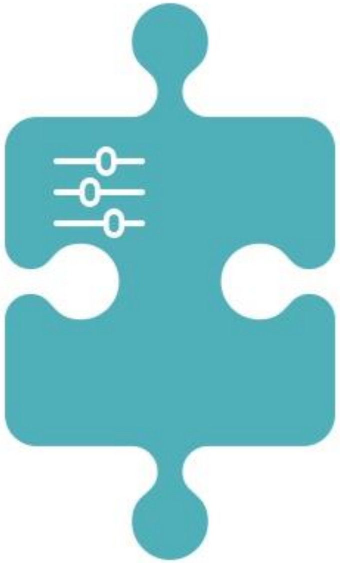
- ICAO *Aviation Security Global Risk Context Statement* (Doc 10108 – Restricted)
- ICAO Global Cyber Risk Considerations (expected in 2024)
- ICAO *Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones* (Doc 10084)
- ICAO Risk Management Workshop
- UNOCT/ICAO Threat Assessment Models Project
- ICAO *Aviation Security Manual* (Doc 8973 – Restricted)
- ICAO *Aviation Security Oversight Manual – The Establishment and Management of a State Aviation Security Oversight Programme* (Doc 10047)

*Not restricted to ICAO resources as other material may also be utilized

What can State do?

Global Priority 1

Enhance risk awareness and response



1. Up-to-date framework and clearly established risk management methodology
2. Timely reporting of AUI to ICAO
3. Appropriate training for those conducting risk assessments and provision of necessary tools to carry out the assessments
4. Global RCS taken into the account when conducting national risk assessments with a holistic aviation perspective and appropriate impact assessments
5. Adjust relevant elements of their NCASP, as necessary and required, based on national risk assessments
6. Review and amend screening and security controls in light of risk assessments
7. Establish and implement a comprehensive cyber risk management framework (across civil aviation domains)

Discussion and Questions