ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

A UN SPECIALIZED AGENCY

SAFE SKIES.
SUSTAINABLE FUTURE.

Convention on International Civil Aviation (Chicago Convention)

- Signed on 7 December 1944 in Chicago by 52 States, and entered into force on 7 April 1944 (when ratified by 26 States)

- Preamble of the Convention:
  - WHEREAS the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a threat to the general security; and
  - WHEREAS it is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the peace of the world depend
  - THEREFORE, the undersigned governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically

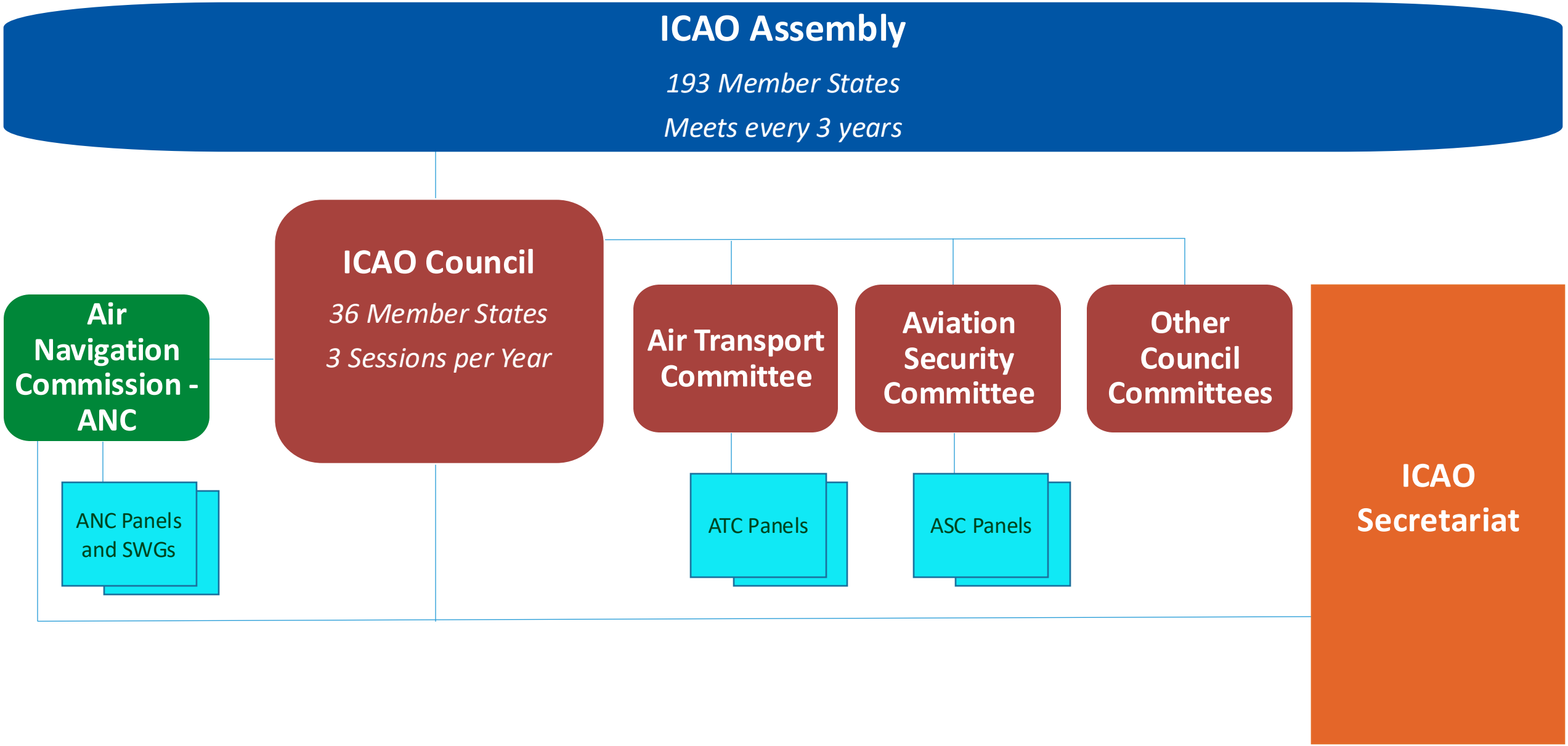
International Civil Aviation Organization – ICAO

- Provisional International Civil Aviation Organization (PICAO) was established on 6 June 1945, pending the ratification of the Convention, and functioned until 5 March 1947.
- In October 1947, ICAO became a Specialized Agency of the United Nation.

International Civil Aviation Organization – ICAO

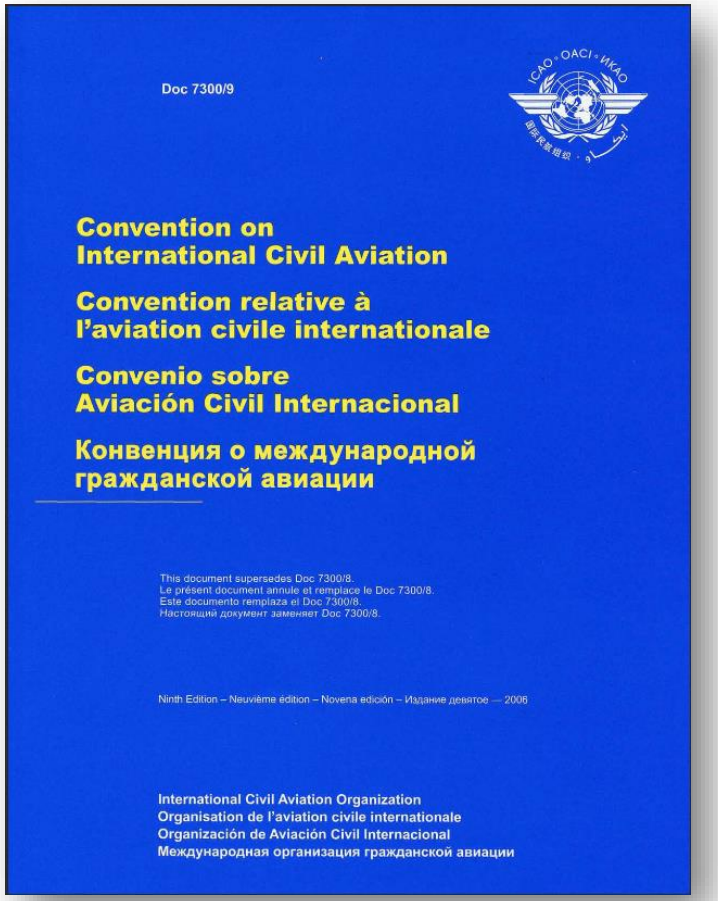
- Headquartered in Montreal – Canada
- Seven Regional Offices and One Sub-Regional Office around the world.
- 193 Member States.
- Issuing Conventions, Protocols, Resolutions, and Standards and Recommended Practices (SARPs)
- **19 Annexes** to the Chicago Convention
- Procedures for Air Navigation Service (PANS)
- Guidance Material.
- Auditing of States: Safety Oversight (USOAP – CMA) and Security (USAP – CMA).
- Providing assistance, training and capacity building to States.

ICAO Structure



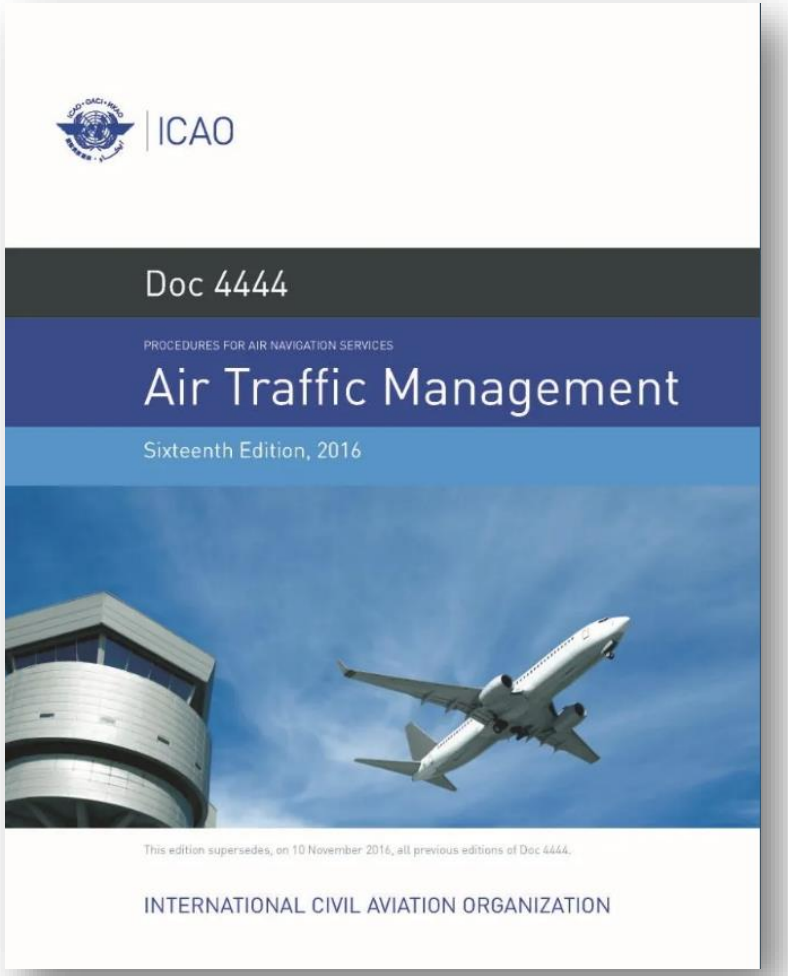
Annexes to the Chicago Convention

Annex 1	Personnel Licensing
Annex 2	Rules of the Air
Annex 3	Meteorological Service for International Air Navigation
Annex 4	Aeronautical Charts
Annex 5	Units of Measurement to be Used in Air and Ground Operations
Annex 6	Operation of Aircraft
Annex 7	Aircraft Nationality and Registration Marks
Annex 8	Airworthiness of Aircraft
Annex 9	Facilitation
Annex 10	Aeronautical Telecommunications
Annex 11	Air Traffic Services
Annex 12	Search and Rescue
Annex 13	Aircraft Accident and Incident Investigation
Annex 14	Aerodromes
Annex 15	Aeronautical Information Services
Annex 16	Environmental Protection
Annex 17	Aviation Security
Annex 18	The Safe Transport of Dangerous Goods by Air
Annex 19	Safety Management



Procedures for Air Navigation Services – PANS

- PANS-ABC Abbreviations & Codes (*Doc 8400*)
- PANS-ATM Air Traffic Management (*Doc 4444*)
- PANS-OPS Aircraft Operations (*Doc 8168*)
- PANS-ADR Aerodromes (*Doc 9981*)
- PANS-AIM Aeronautical Information Management (*Doc 10066*)
- PANS-TRG Training (*Doc 9896*)
- PANS-IM Information Management (*Doc 10199*)



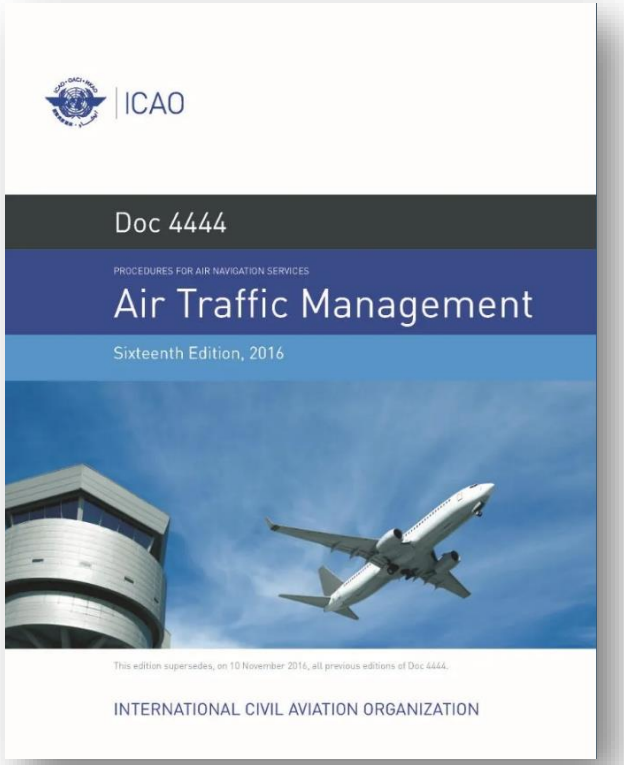
ICAO Publications

Annexes

Contain:

- International Standards
- Recommended Practices

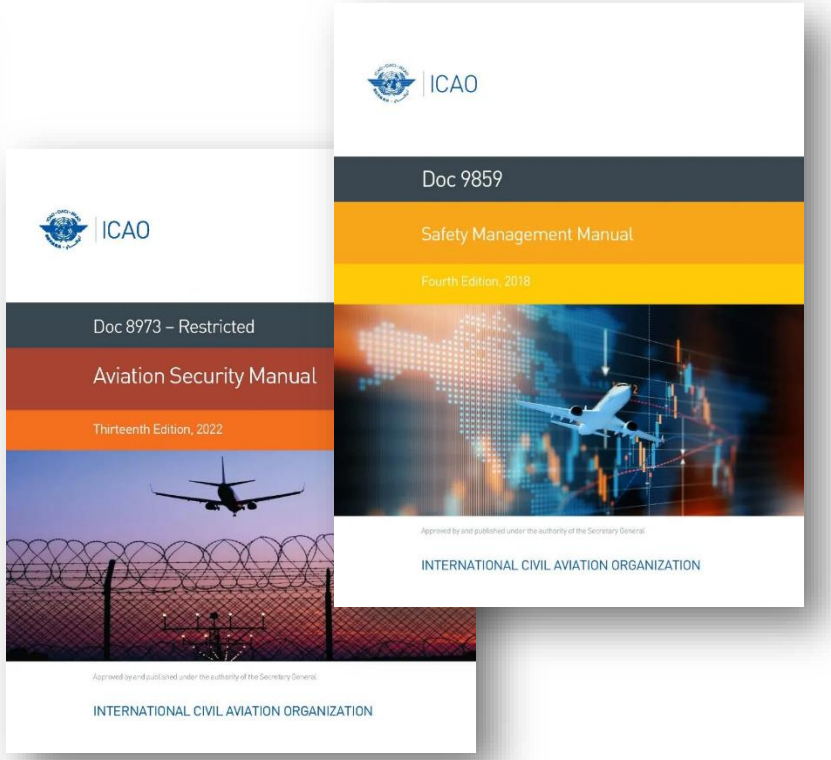
Procedures for Air Navigation Services



Contain:

- Operating procedures
- Technical Material

Guidance Material

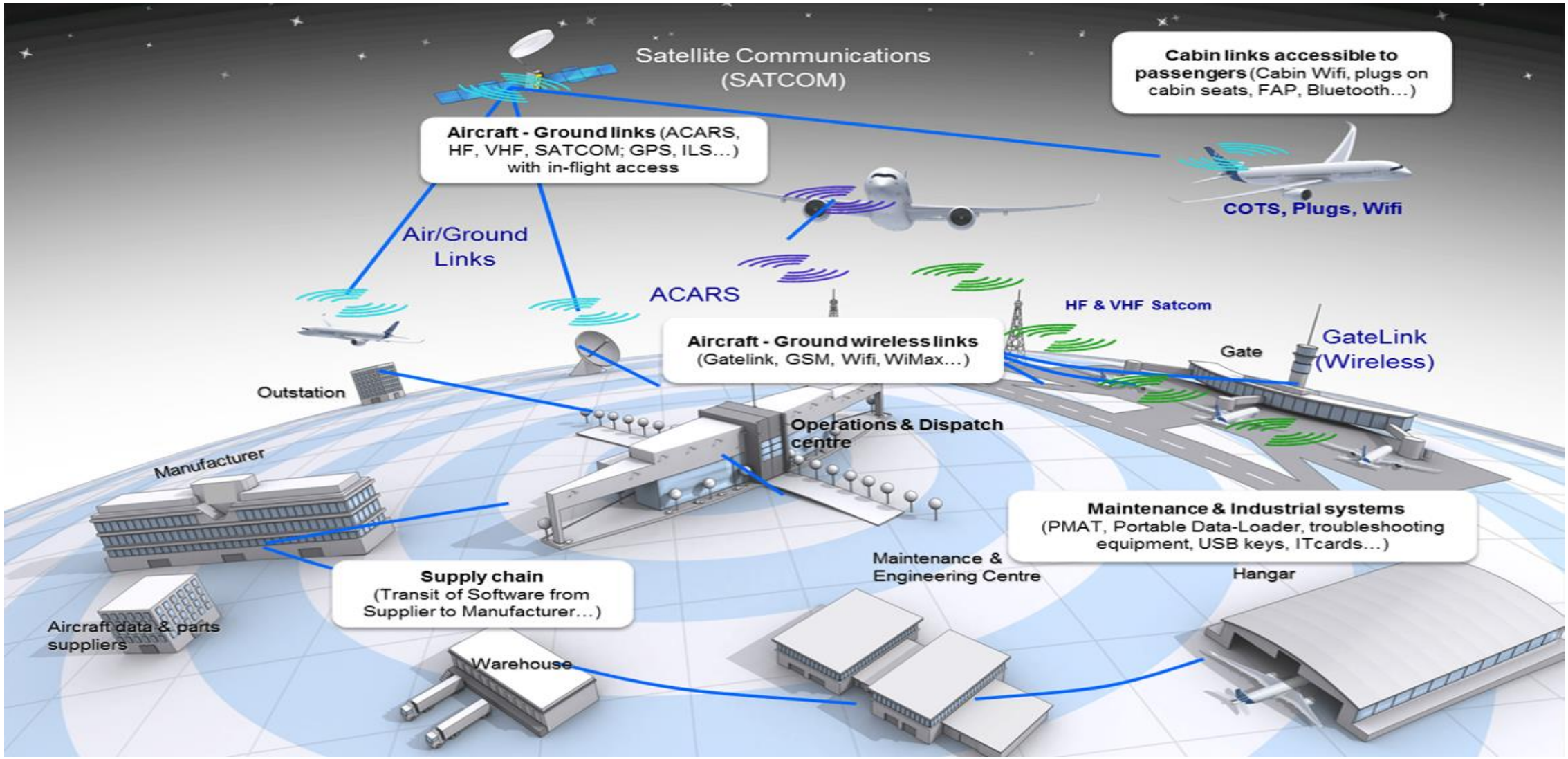


Contain:

- Means of Compliance
- Examples & Best Practices

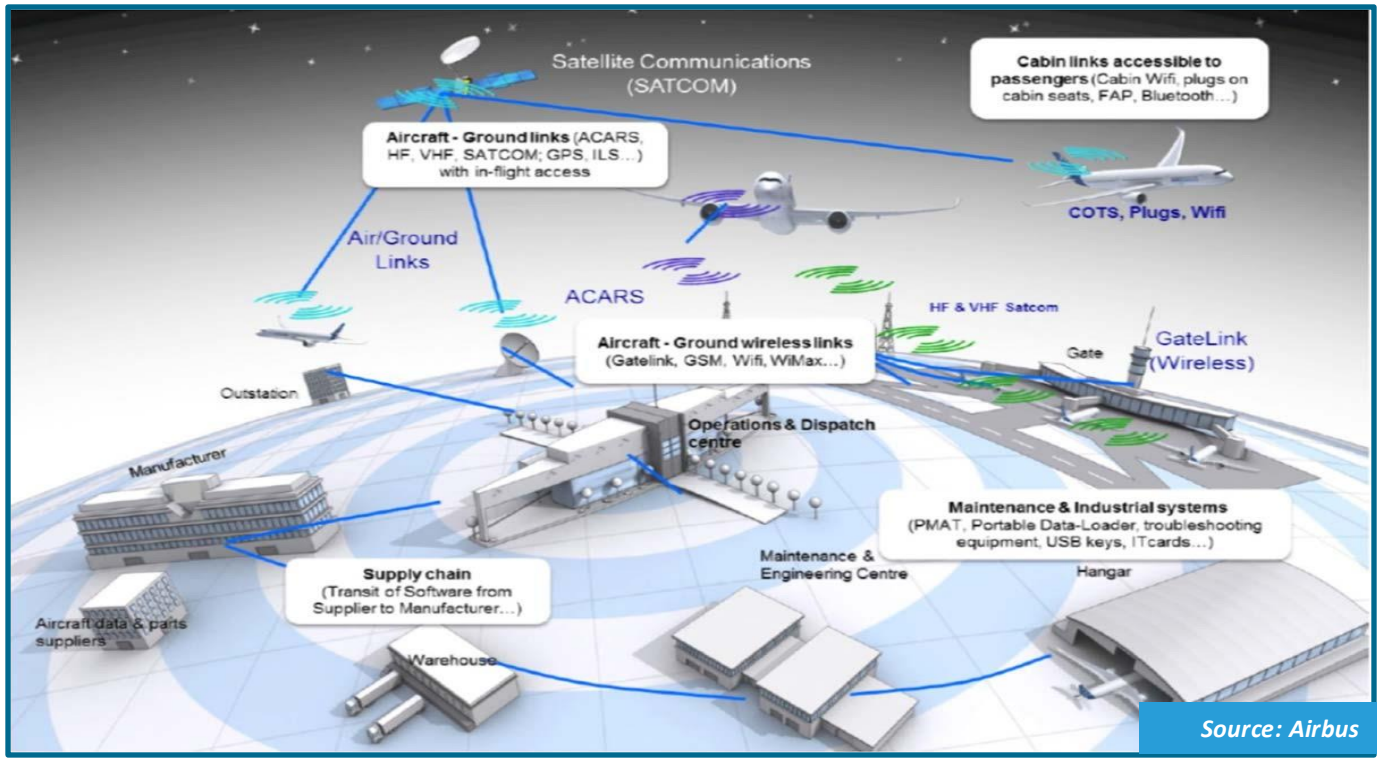
SETTING THE CYBER SCENE

Aviation Ecosystem



Why Cybersecurity in Civil Aviation?

Impact of Technology



Technology facilitates growth of air transport while enhancing its safety, security, efficiency, capacity, and sustainability.

However, connecting aviation systems between stakeholders increases the cyber-threat surface.

Draft Definitions/Glossary of Terms

Aviation Cybersecurity	The body of technologies, controls and measures, processes, procedures and practices designed to ensure confidentiality, integrity, availability, and overall protection and resilience of cyber assets from attack, damage, destruction, disruption, unauthorized access, and/or exploitation.
Cyber Asset	Digital and physical items which have value in terms of business, operations, aviation safety, aviation security, efficiency and/or capacity, such as systems, information, data, networks, devices, software, hardware, processes, firmware, relevant/certified personnel, and other electronic resources.
Cyber Resilience	The ability of a cyber asset to maintain critical functions under adverse conditions or stress, and to recover from those adverse conditions.
Critical Aviation Infrastructure	Assets that are so vital that their incapacity, compromise, or destruction would have a debilitating impact on aviation safety, aviation security, efficiency, and/or capacity.
Cyber Event	Any observable occurrence in a network or system.
Cyber Incident	A single, or a series of cyber event(s) that adversely impacts aviation safety, aviation security, efficiency, and/or capacity.
Cyber Threat	Any potential cyber event that might adversely impact aviation safety, aviation security, efficiency, and/or capacity.
Cyber Risk	Potential for an unwanted outcome resulting from a cyber event.
Cyber Mitigation	Security control(s) that aim at lowering the cyber risk associated with a specific cyber threat or vulnerability, taking into account their impact on aviation safety, aviation security, efficiency, and/or capacity.
Cyber Risk Assessment	Continuous process of cyber risk identification, analysis, and evaluation.
Cyber Risk Management	The continuous process of identifying, mitigating, treating and monitoring cyber threats and risks, according to a risk assessment.

Threats and Vulnerabilities

- **Ecosystem connectivity leads to opportunity for proliferation of effects**
- Insider threats
  - Could be motivated or unwitting
- Information Systems
  - Phishing, connected system attacks
- Movement between networks
- Supply chain impacts
  - 3rd party software vendors and hardware vendors
  - Software and firmware updates
- Connected systems (e.g. service kiosks, maintenance terminals, test equipment) and other media (EFBs)
- Disruptions to GNSS and Timing
- Other attack vectors

Areas of Concern for Civil Aviation

- IT network crashes/lack of disaster recovery plans
- Confidentiality, Integrity, and Availability of Data
  - Flight planning systems
  - Electronic Flight Bags
  - Airline/Airport Networks (Ground side, Air side)
  - Software parts
- Cyber hygiene across entities
  - Phishing
  - Malware insertion
- GNSS and Timing Disruption
  - Spoofing
  - Jamming
- General lack of encryption or authentication
- Incident management across regions/borders

Typical Cyber Attack Process

- Reconnaissance: Attacker gains information on a target and assesses its vulnerabilities
- Initial Access/Compromise: Attacker successfully executes malicious code to exploit vulnerabilities and gain access
- Entrenchment: Attacker establishes foothold of control over system
- Internal Reconnaissance: Attacker explores environment to gain better understanding of environment
- Move Laterally: Attacker uses their access to move from system to system
- Abuse: Attacker manipulates, extracts, compromises or otherwise conducts actions to achieve their goal or desired effects.

Cybersecurity Challenges

- How is cybersecurity addressed across States and stakeholders?
- What (legislatively) should be done by whom?
  - To what extent can standards be applied?
  - Legal frameworks and requirements
  - Audit and compliance validation
- How can cyber information be shared amongst stakeholders?
- How can incidents be recognized and managed across borders?

Aviation Cyber Provisions

- International
  - Beijing Instruments
  - ICAO Annex 17
  - Other ICAO Annexes and PANS
- Regional
  - European NIS2 Directive
  - European Part-IS
- National
  - Various frameworks
  - Scope and level of impact vary by State

Legal Instruments

Beijing Convention 2010

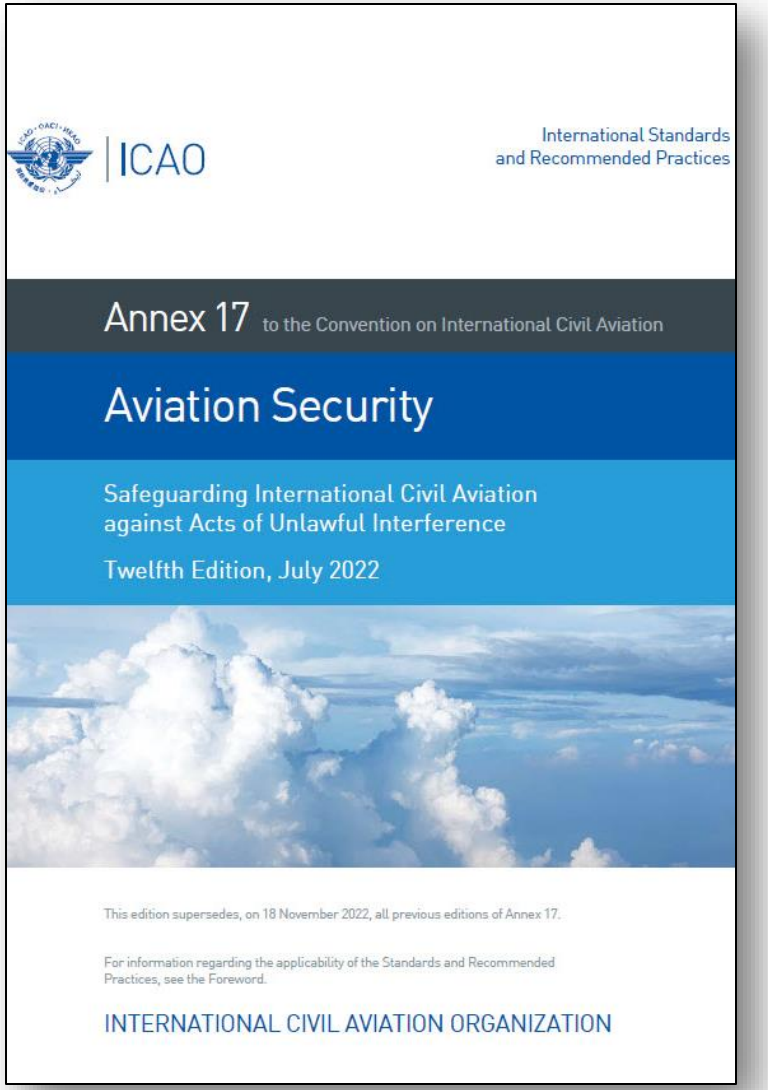
- Defines air navigation facilities to include signals, data, information or systems.
- Such facilities could be directly applicable to cyber means of carrying an attack.

Beijing Protocol 2010

- Broadens scope to aircraft in service instead of in flight, adds or by any technological means to Article 1.
- No requirement for the offender to be on board.

ICAO Standard & Recommended Practice on Cybersecurity

- **Annex 17 to the Chicago Convention – Aviation *Security***
- **Standard 4.9.1**
  - Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation **identify** their critical information and communications technology systems and data used for civil aviation purposes and, **in accordance with a risk assessment**, **develop and implement**, as appropriate, measures to protect them from unlawful interference.
- **Recommended Practice 4.9.2**
  - Recommendation— *Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.*



ICAO

Compliance Challenges:
USAP-CMA Audit Results for A17 Standard 4.9.1

- 54 States Documentation-Based Audits:
  - 15% - No requirement for entities to identify their critical infrastructure and develop, in line with risk assessment, measures to protect this critical infrastructure.
  - 26% - No definition for entities' responsibilities in relation to aviation cybersecurity.
  - 41% - No criteria for the protection of critical infrastructure from unlawful interference.
- 35 States On-Site Audits:
  - 60% - No implementation of consistent and effective cybersecurity measures.

Other ICAO Annexes and PANS

- Cyber-related provisions are in many other annexes, without specifically being referenced
  - Annex 1
  - Annex 6
  - Annex 10
  - Etc…
- Cyber-related provisions for information security are also in PANS-IM
  - Information security framework for SWIM

Regional Legislation - NIS2

- Builds upon 2016 NIS directive for critical infrastructure in Europe
- NIS2 expands the scope of organizations to which the original directive applied
- It places obligations on Member States and individual companies in critical sectors
- Both transformation and digital trust providers are listed as critical infrastructure
- In effect since 2023, deadline for transposition into national law was October 2024
- Heavy penalties for non-compliance (up to EUR 10M or 2% of global revenue)

Regional Legislation - Part-IS

- Requirements for the identification and management of information security risks which could affect information and communication technology systems and data used for civil aviation purposes
- Sets requirements for detection of information security events, responding to, and recovering from incidents to a level commensurate with their impact on aviation safety
- Risk-driven approach
- Effective October 2025

Sharing - Steps for a Cyber Information Sharing Plan

1. Define Cyber Information Sharing Policy
2. Establish Regulatory and Contractual Requirements
3. Identify human, technical, and financial resources required
4. Scope sources and tools, maintain a POC network, test systems, launch, and continuously improve.

Communication Tools that Can be Used

Sharing - Important Considerations

ASSESS THE SOURCE

ANALYZE PLAUSIBILITY/CREDIBILITY OF THE INFORMATION

ANALYZE RELEVANCE TO ORGANIZATION, INFORMATION SHARING COMMUNITY, AND AVIATION ECOSYSTEM

Cyber Information Sharing: Traffic Light Protocol (TLP)

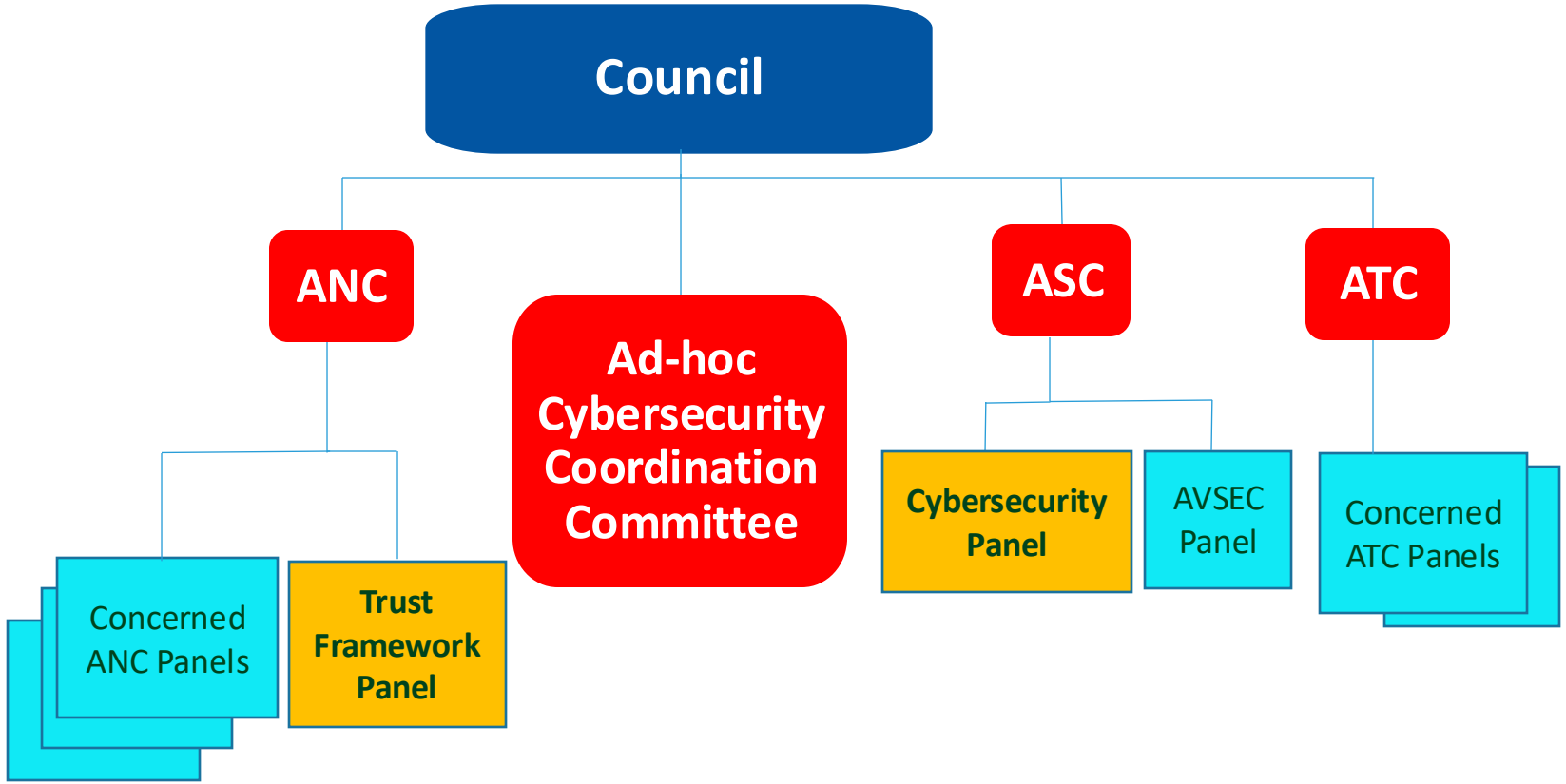
TLP:CLEAR	marking does not constraint the dissemination of the received information to anyone through any medium.
TLP:GREEN	Information can be shared within the aviation community.
TLP:AMBER	Information can be shared on a need-to-know basis within the organization of the recipient and its clients.
TLP:AMBER +STRICT	Information can be shared on a need-to-know basis only within the organization of the recipient.
TLP:RED	marking limits disclosure of the information to the specific recipient(s) with no further distribution at all, these two markings are not discussed in this section.

ICAO'S CYBER WORK

ICAO Cyber Work Areas

- Internal Organization
- Cybersecurity Strategy
- Cybersecurity Action Plan
- PANS-IM
- High-level Guidance Materials
- Specific Guidance
- Technical Guidance
- Inter-level Guidance Coordination (“Guidance flow”)

Internal Organization



ICAO

History of Cyber-related ICAO Groups

- ICAO Council established a group to study ways of managing cyber-related work at ICAO
- As part of this work, the Council decided that the former Secretariat Study Group on Cybersecurity (SSGC) should be transformed into a panel under the Aviation Security Committee and the Trust Framework Study Group (TFSG) should be formally integrated into the ANC panel structure
  - During its 219th session, the ANC decided to establish the TFSG as an independent panel, and requested draft terms of reference, membership criteria and job cards to be presented during the 220th session
- An Ad-hoc Cybersecurity Coordination Committee (AHCCC) was also established to bring relevant panels and expert groups together to ensure high-level coordination of cyber activities

AHCCC

- Function
  - monitors the implementation of the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan and oversee the development of updates thereto
  - develops and maintains a comprehensive ICAO Aviation Cybersecurity Work Programme, to coordinate ICAO aviation cybersecurity work across all aviation domains
  - advises the Council on policy, strategic direction, priorities and activity planning and other aviation cybersecurity issues, as required
- Outcomes of last meeting:
  - Updates by IMP and TPF on SWIM and Trust Framework topics
  - SMP as a new Member updated on current work in progress
  - Detailed technical updates on securing:
    - Comms infrastructure (DCIWG of CP)
    - Navigation infrastructure, highlight on GNSS spoofing (NSP)
    - C2-Link and other included security features (RPAS Panel).

Panels of the Air Navigation Commission

- A Panel is a group of experts formed by the ANC and is under its direct supervision
- Panels are subject to the provisions found in *Doc 9874 - Directives for Panels of the Air Navigation Commission*
- Panels of the Aviation Security Committee and Air Transport Committee operate under their own rules

Panels of the Air Navigation Commission (ANC)

- The purpose of a panel of the ANC is to advance, *within specified time frames*, the solution of *specialized problems* or the development of standards for the *planned evolution of air navigation* which cannot be advanced within the ANC or established resources of the Secretariat.

Panel Terms of Reference

- The ANC shall establish the panel's terms of reference
- The terms of reference shall define clearly and concisely the *nature and scope* of the work assigned to the panel and *specify the objectives* sought by the ANC
- The ANC shall revise the terms of reference when this becomes necessary

Example - TFP Terms of Reference

Background Describe the background of the panel including an outline of any changes to this current version.	The evolution of systems for data and information processing, raised concerns in the aviation community regarding the effectiveness of existing standards, procedures and processes to ensure the risks involved in the exchange of messages in a digital environment are kept at an acceptable level. Cyber-related events are recognized by the aviation community as capable of severely disrupting the safe and efficient provision of aviation services and the reduction of the cyber-attack surface of these systems is a common goal for all stakeholders. ICAO began exploring how to enable the secure, safe efficient, and resilient exchange of information in 2015, leading to AN-Conf/13 Recommendation 5.4/1 on Cyber Resilience. This led to the formation of the Trust Framework Study Group (TFSG) in the ANC's 210th Session of the ANC. The TFSG conducted six meetings to advance the work of facilitating the establishment of a global trust framework to enable the safe, secure and resilient exchange of information. Following the decision of the ICAO Council taken during the eleventh meeting of its 222nd Session regarding the governance of cybersecurity within ICAO (C-DEC 222/11), the ANC decided to evolve the TFSG into an independent panel (AN Min. 219-6 refers).

Scope	The panel:
Describe the boundaries of the panel in terms of aviation specialties and the work programme.	• Develop a common set of principles, policy and guidance, and a transition strategy for a globally harmonized framework that will enable trusted ground-ground, air-ground and air-air exchange of data and information amongst States, relevant stakeholders, airspace users, service providers and new entrants such as unmanned aircraft systems , remotely piloted aircraft systems , etc. with the level of resilience and interoperability needed to support increased capacity and efficiency for the continued safe operation of the civil aviation system; and • Consider and incorporate current and future needs for States, relevant stakeholders, airspace users, service providers and new entrants in the aviation system while ensuring the globally harmonized trust framework takes into account human-system interaction factors and relevant technologies, including the Internet infrastructure, for the exchange of information in support of air traffic management, airport operations and flight operations.

Required Competencies Detail the desired knowledge, skills, and experience of the panel members.	The panel should be composed of experts that provide the following competencies: • Aviation and non-aviation policy, technical and operational experts involved in the development and operation of identity management systems, information assurance policies and data exchange networks; • Familiarity with the interoperability requirements necessary to develop and sustain a global trust framework environment; and • Technical and policy experts supporting systems enabling trusted information exchange, Internet governing bodies, and other technical standards organizations.

Objective(s) The strategic objectives of the panel are to be clearly stated. Specific tasks shall be provided on individual job cards.	• Develop, address and maintain provisions and guidance materials to support globally harmonized frameworks enabling the trusted exchange of data and information amongst States, relevant stakeholders, airspace users, service providers and new entrants. • Ensure the needs and requirements of States, relevant stakeholders, airspace users, service providers and new entrants are duly considered in all deliberations, with a focus on converging to common integrated solutions and exploration of technological innovations. • Explore and define operational and efficiency drivers, requirements and benefits of trusted systems. • Develop governance principles, policy, procedures and requirements for establishing digital identities for supporting trusted exchange of information amongst States, relevant stakeholders, airspace users, service providers and new entrants, and to promote these concepts with all relevant stakeholders.

ANC Work Programme

- The work programme shall comprise *a list of detailed items*, with each item individually approved by the ANC, within the assigned terms of reference
- The ANC will normally include a *statement of the problem* requiring resolution, *required actions, deliverables and timescales*
- The ANC shall revise the work programme as necessary, normally after each substantive phase of the panel's work, such as following a meeting

ANC Job Cards

- Related tasks and deliverables are grouped into a document called a Job Card (JC)
- JCs are the primary vehicle by which ANC exercises control and direction over panels
- The collection of JCs constitutes the work programme of the panel and is approved by the ANC
  - ANC approves **all** new and amendments to JCs

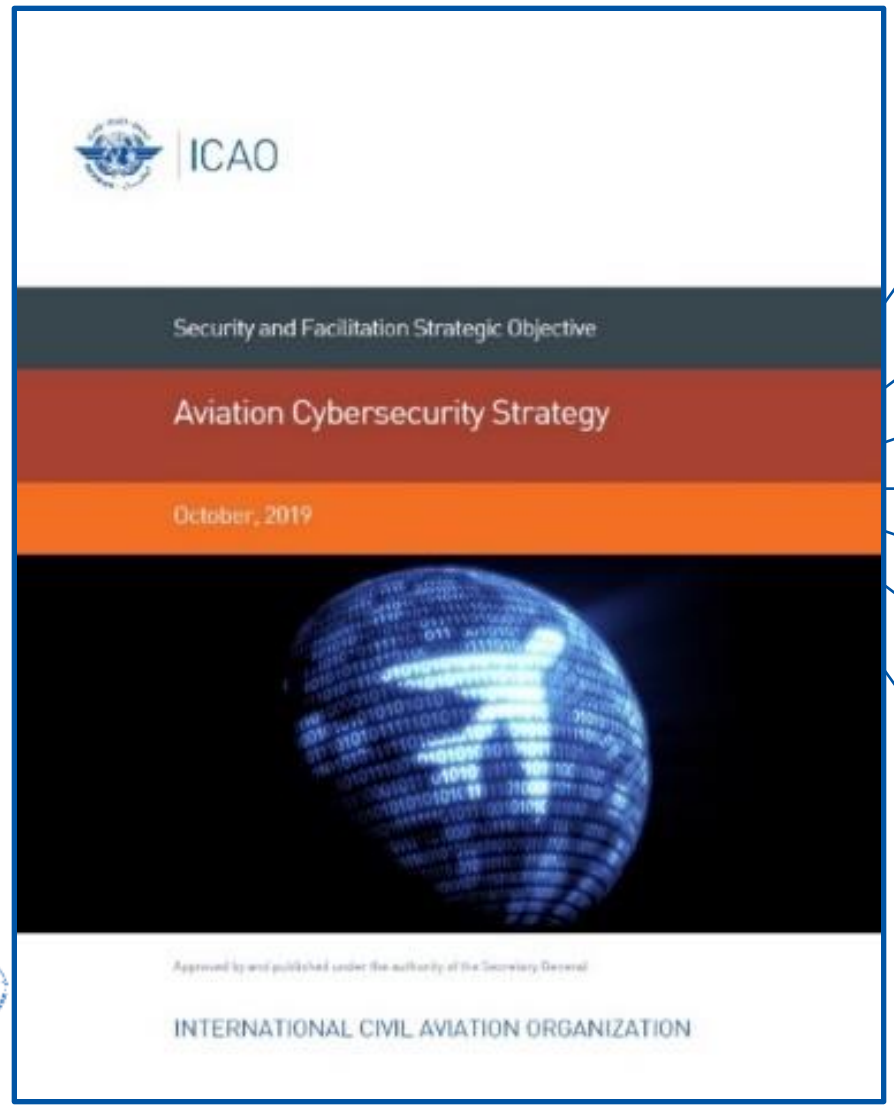
Job Card Contents

- JCs follow a standard template
- JCs specify the from, where, why, how and when for each work item/package of the panel

Job Card Composition

Item	Description
Source	Source of the JC (i.e. Council, ANC, Assembly, High-level meeting, Panels, Regional Office, AN-Conf. etc.)
Problem Statement	Define the problem in a concise and accurate way, ideally without mentioning a solution
Specific Details	Provide additional details to describe the context of the problem, most importantly: why does ICAO need to do this?
GANP/GASP Link	Reference to ASBU elements and KPIs or GASP goals
Expected Benefits	Describe benefits including the potential support of the ICAO Strategic Objectives
References	Provide a reference to the document(s) relating to the problem statement and actions (eg. conference/Assembly reports, etc…)
Primary Expert Group:	Expert group responsible for the delivery of all WPEs
Work programme elements	List of individual actions/deliverables to satisfy the problem statement

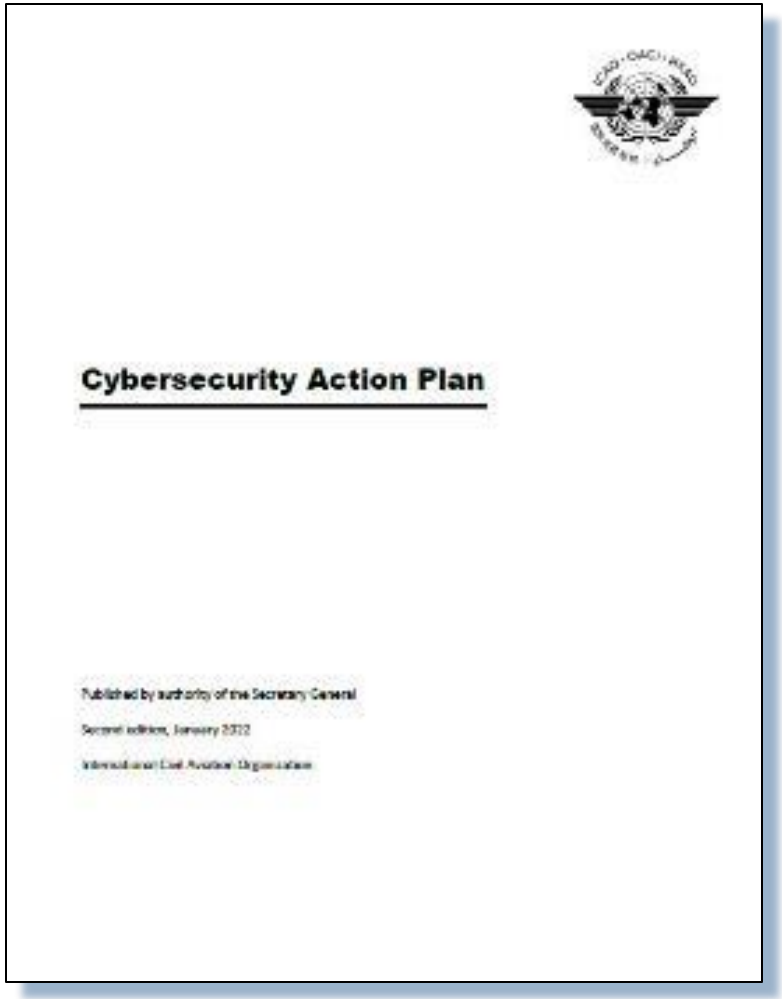
ICAO Aviation Cybersecurity Strategy



- International Cooperation
- Governance
- Effective Legislation & Regulations
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building, Training, & Cybersecurity Culture

https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

Cybersecurity Action Plan



First Edition published in November 2020

Second Edition published in January 2022

Available on ICAO Public Website

Provides the Foundation for ICAO, States and stakeholders to work together

Develops the **7 Pillars** of the Aviation Cybersecurity Strategy into **32 Priority Actions**, which are further broken down into **51 Tasks** to be implemented by ICAO, States, and Stakeholders

https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

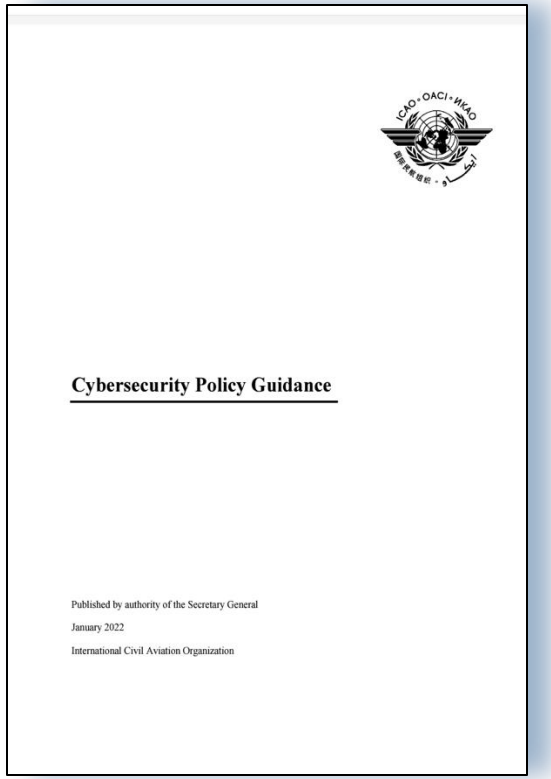
Cybersecurity Action Plan (Example)

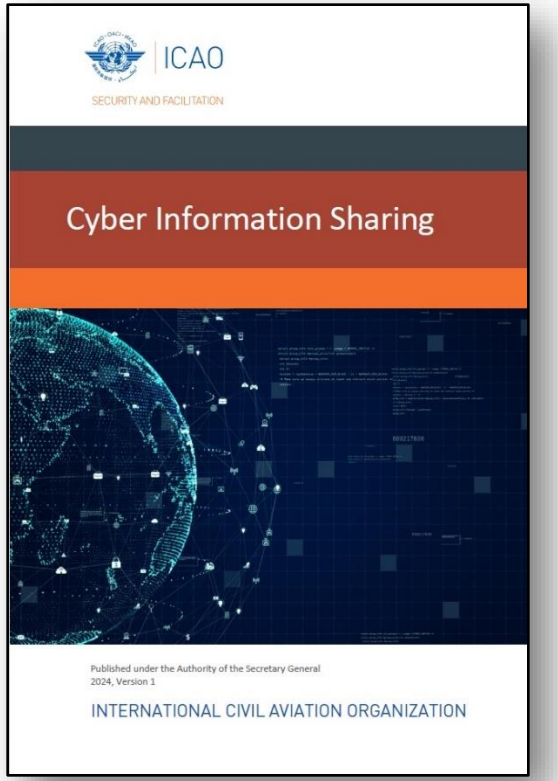
Action #	By	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 0.1	ICAO, Member States, and Industry	ICAO to develop a model Cybersecurity Policy for reference by Member States and Industry when developing their own national/organizational policies.	The model is available to Member States and Industry.	High	2021
CyAP 2.1	ICAO and Member States	Establish a governance structure in the civil aviation cybersecurity field.	Identification of adequate governance structure(s) for civil aviation cybersecurity.	N/A	2021-2023
CyAP3.1	Member States	Member States to ratify Beijing instruments.	Number of States having ratified the Beijing instruments.	High	Ongoing
CyAP 2.5	ICAO	ICAO to include cybersecurity in regional and global plans to ensure the safety, security, and resilience of aviation.	Updated Plans published.	N/A	2022-2023
CyAP 6.1	Member States, and Industry	Member States to establish targets and minimum levels of functionalities essential to the civil aviation sector. Industry to apply the targets developed.	Publish a list of targets and minimum acceptable levels of functionalities for aviation continuity.	High	2022 - 2023

PANS-IM

- PANS-IM contains material that supports the transition towards a global air navigation system network, as described in the Global Air Navigation Plan (GANP, Doc 9750)
- Focus is on information services for ground-to-ground information exchanges based on the principles, benefits and components described in the Manual on the System-wide Information Management Concept (Doc 10039), to establish SWIM as a key enabler of the Global Air Traffic Management Operational Concept (Doc 9854)
- Includes requirements for an information security framework to have a common understanding on the level of protection of the information and to provide end-to-end information security in a scalable approach
  - Manual on Aviation Information Security (Doc 10204)
- Became effective 28 November 2024

High-level Cybersecurity Guidance





https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Future Cybersecurity Policy Guidance

- Glossary of terms
- State policy and regulatory guidance
- Interrelation of SMS, SeMS and ISMS
- Incident Response
- Cybersecurity Supply Chain
- Cybersecurity Training Programme Considerations
- And more…

Specific Guidance – Identity Management and Information Security

- Doc 10169 – Aviation Common Certificate Policy
  - Provides a reference certificate policy for implementers of PKI-based solutions
  - Catalogue of certificate profiles for civil aviation and aeronautical communications applications
  - Available in 2025

- Doc 10204 – Manual on Aviation Information Security
  - Provides implementation guidance on information security frameworks
  - Includes a risk assessment process for considering safety and information security risks
  - Available soon

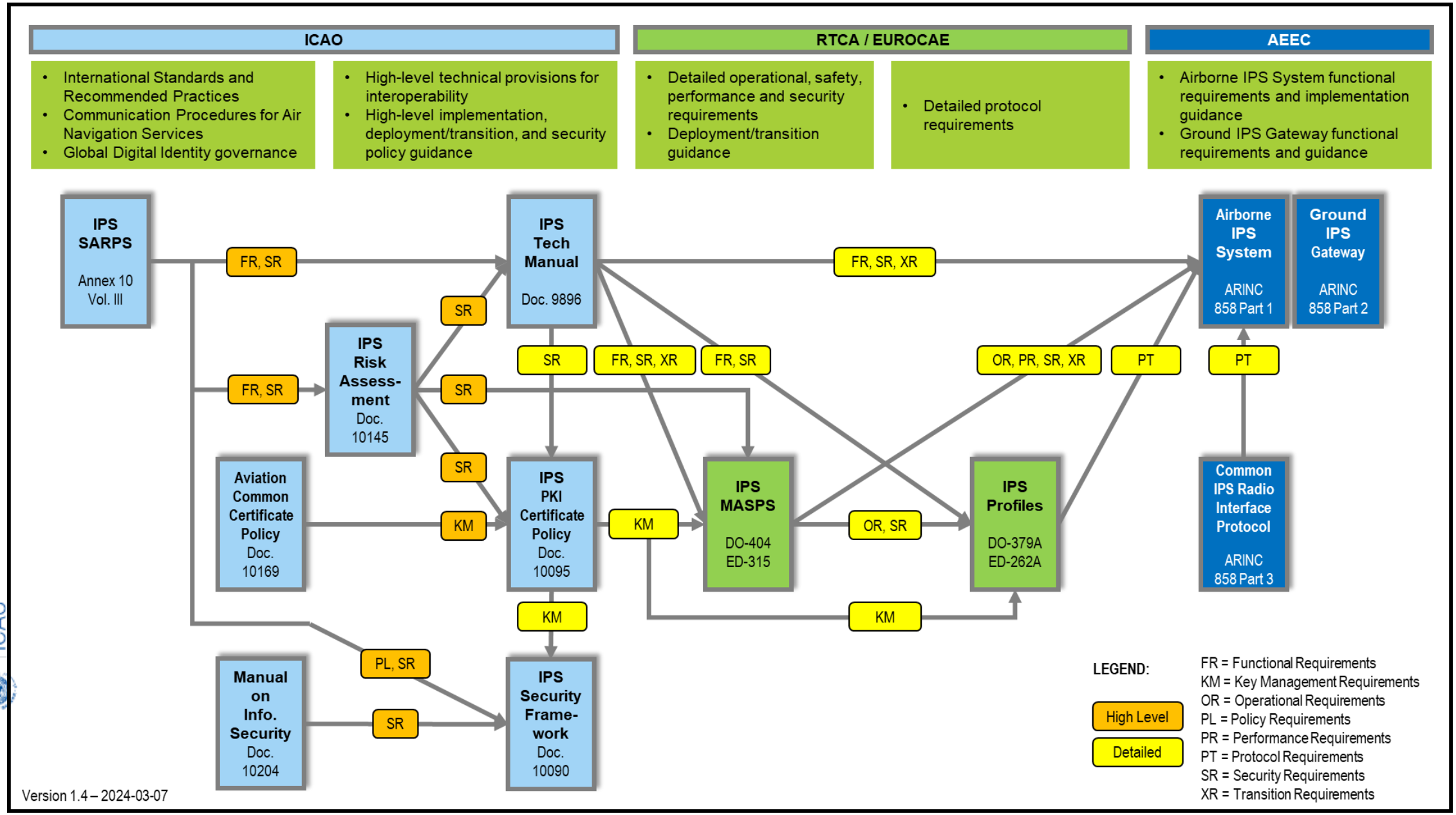
Technical Guidance

- Doc 10090 – Manual of Security Services for Aeronautical Communications
  - Guidance on information security for air/ground aeronautical communications
  - Based on Doc 10204 – Manual on Information Security
- Doc 10095 – Manual of the PKI Policy for Aeronautical Communications
  - PKI implementation guidance for air-ground communications requiring PKI systems
  - Based on Doc 10169 – Aviation Common Certificate Policy
- Doc 10145 – Manual of Security Risk Assessment for Aeronautical Communications
  - Provides a generic security risk assessment for IPS systems in the context of ATS datalink and Aeronautical Operational Control safety data communications

Standards Development Organizations

- SDOs play an important role in technical guidance development
- Aviation-specific SDOs
  - RTCA
  - EUROCAE
  - Airlines Electronic Engineering Committee (AEEC)
- Non-aviation SDOs
  - International Telecommunications Union (ITU)
  - American Society for Testing and Materials (ASTM)
  - Internet Engineering Task Force (IETF)
  - *International Organization for Standardization (ISO)*
  - *Institute of Electrical and Electronics Engineers (IEEE)*
  - *National Institute of Standards and Technology (NIST)*
  - *Society of Automotive Engineers (SAE)*

Guidance Flow



Guidance Flow -
Risk Interrelation Methodology

Step 0: Identify Critical Systems, data and information.

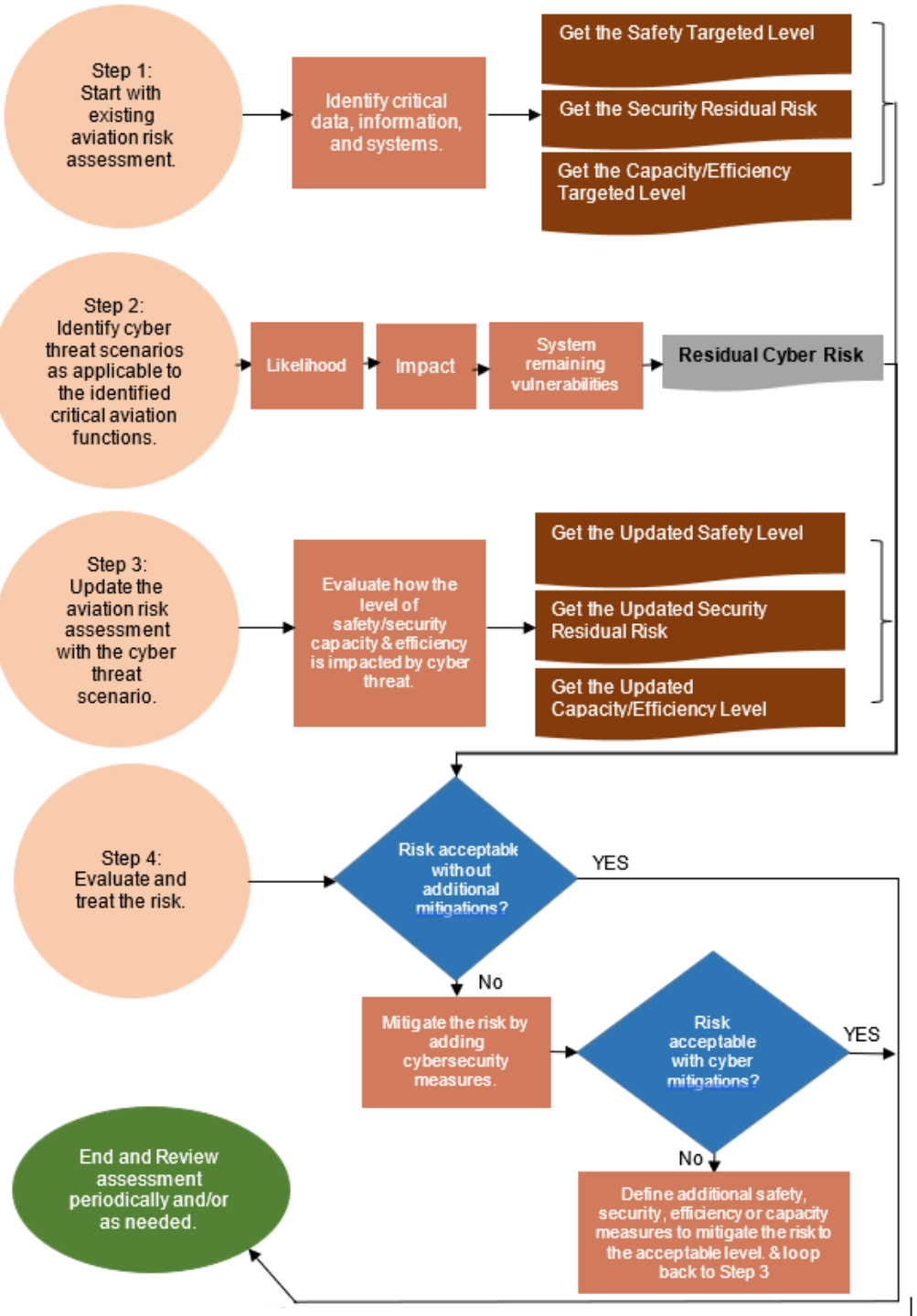
Step 1: Begin with Existing Aviation Risk Assessment.

Step 2: Identify & Assess Cyber Threat Scenarios affecting Critical Infrastructure.

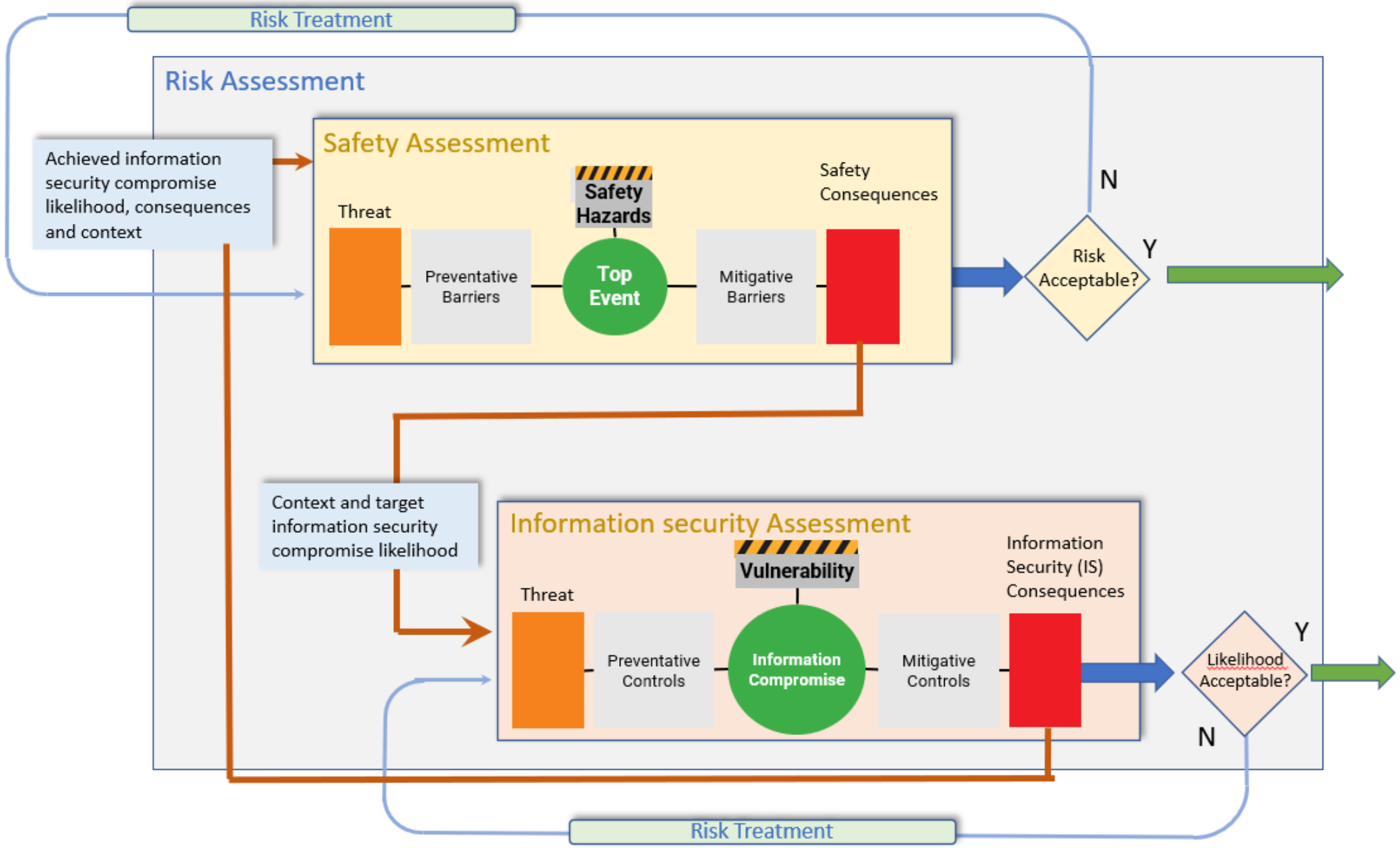
Step 3: Update Aviation Risk Assessment to Include Cyber Risk Assessment.

Step 4: Evaluate and Mitigate.

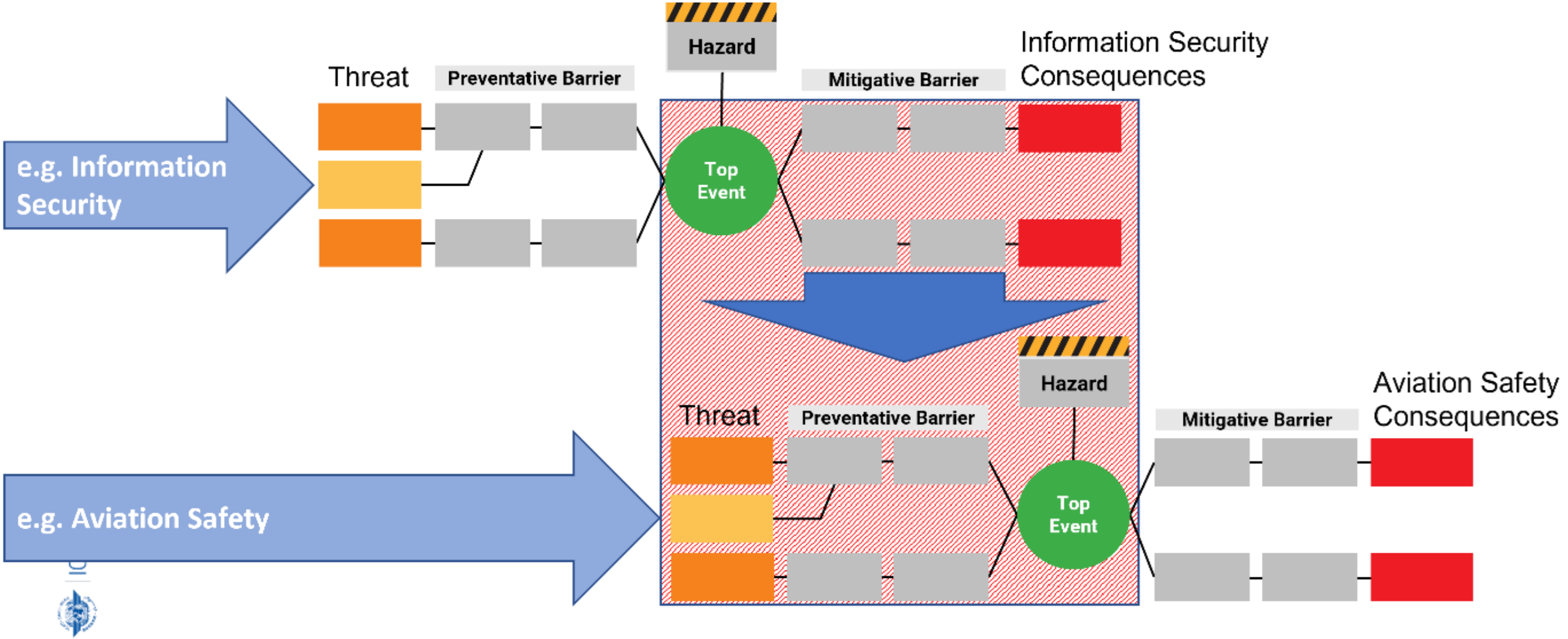
Step 5: Monitor and Review



Specific Guidance - Risk Interrelation Process



EASA Part-IS Risk Management



Summary

- Cyber in aviation is complex and multifaceted
- Aviation's increasing interconnectivity brings both opportunities and challenges
- A broad, coordinated understanding of cyber issues is critical
- Cyber is a team sport – nobody can do it alone
- Collectively we can rise to the challenge

Thank You!

ICAO