SAFE SKIES.
SUSTAINABLE FUTURE.

Overview of ICAO Policy Work on Aviation Cybersecurity

Rashad Karaky

Aviation Cybersecurity Officer
International Civil Aviation Organization (ICAO)

ICAO

Agenda

- ICAO, Its Mandate, and Provisions
- Why Cybersecurity in Civil Aviation and the role of ICAO
- Definitions/Glossary of Terms
- ICAO Standard & Recommended Practice on Aviation Cybersecurity
- ICAO Assembly Resolutions on Aviation Cybersecurity
- International Legal Instruments
- The Aviation Cybersecurity Strategy and Action Plan
- Aviation Cybersecurity Guidance Material
  - Governance
  - Policy
  - Cyber Risk Management
  - Cyber Information Sharing
  - Cybersecurity Culture
  - In the Pipeline
- ICAO Training & Capacity Building Initiatives

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;

Convention on International Civil Aviation (Chicago Convention)

Article 44:
Objectives

The aims and objectives of **the Organization** are to develop the principles and techniques of international air navigation and to foster the planning and development of international air transport so as to:

a) Insure the safe and orderly growth of international civil aviation throughout the world;
b) Encourage the arts of aircraft design and operation for peaceful purposes;
c) Encourage the development of airways, airports, and air navigation facilities for international civil aviation;
d) Meet the needs of the peoples of the world for safe, regular, efficient and economical air transport;
e) Prevent economic waste caused by unreasonable competition;
f) Ensure that the rights of contracting States are fully respected and that every contracting State has a fair opportunity to operate international airlines;

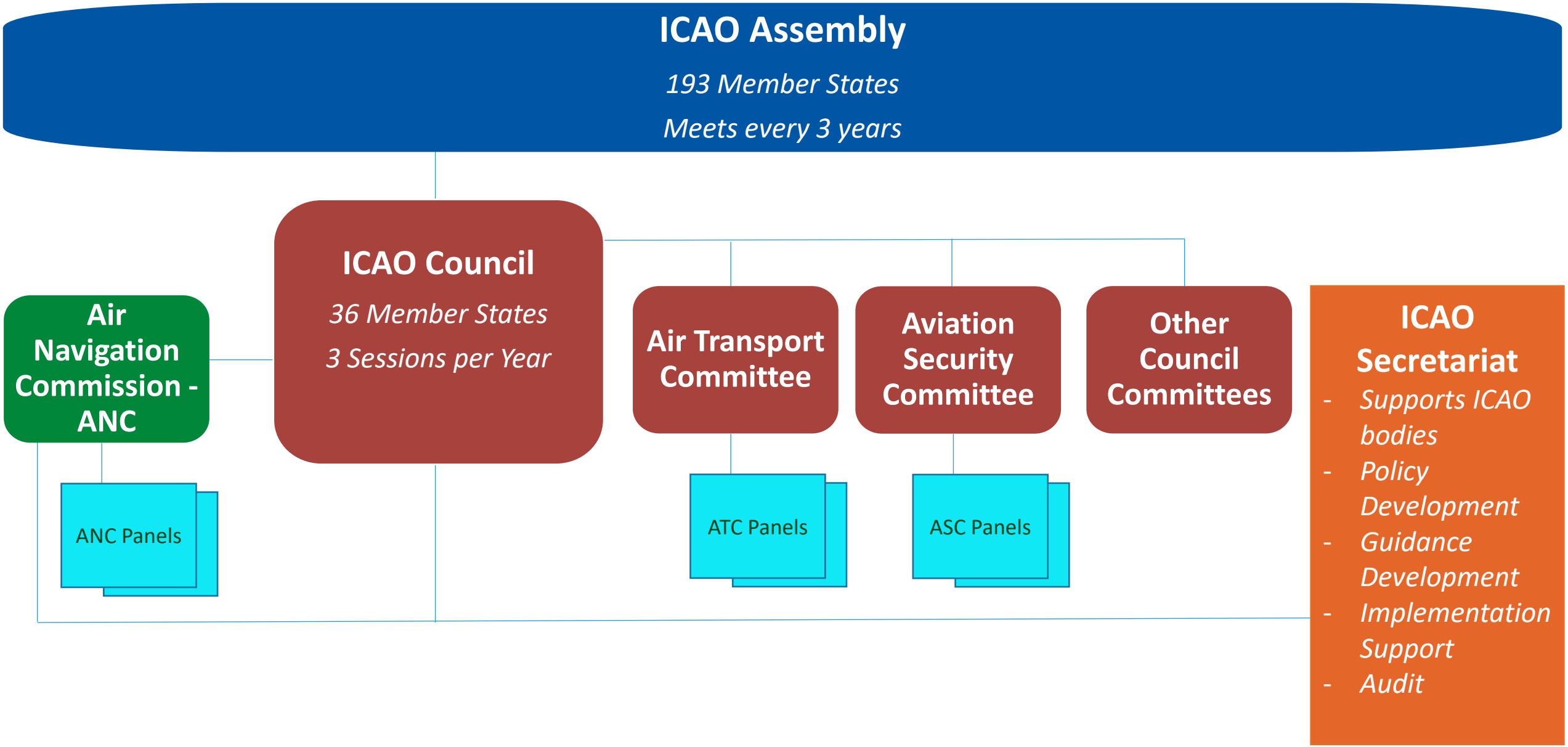
International Civil Aviation Organization – ICAO

- 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) contained in **19 Annexes** to the Chicago Convention, Procedures for Air Navigation Service (PANS), and Guidance Material.
- Auditing of States: Safety Oversight (USOAP – CMA) and Security (USAP – CMA).
- Providing assistance, training and capacity building to States.

ICAO Structure



ICAO Strategic Objectives

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

Standards & Recommended Practices - SARPs

- **Standards:**

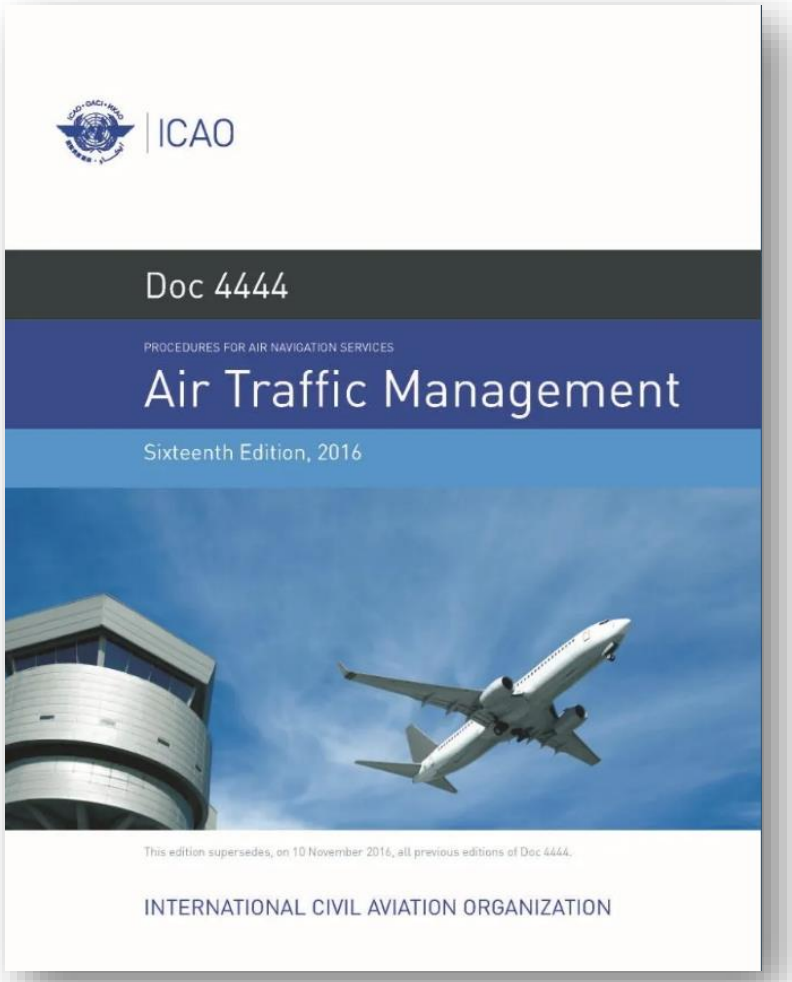
Any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as necessary for the safety or regularity of international air navigation and to which Contracting States will conform in accordance with the Convention; in the event of impossibility of compliance, notification to the Council is compulsory under Article 38.

- **Recommended Practices:**

Any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as desirable in the interest of safety, regularity or efficiency of international air navigation, and to which Contracting States will endeavour to conform in accordance with the Convention.

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*)



Procedures for Air Navigation Services – PANS

➢ **PANS standards:**

- PANS contain, for the most part, operating procedures regarded as not yet having attained a sufficient degree of maturity for adoption as SARPs, as well as material of a more permanent character which is considered too detailed for incorporation in an Annex, or is susceptible to frequent amendment, for which the processes of the Convention would be too cumbersome.

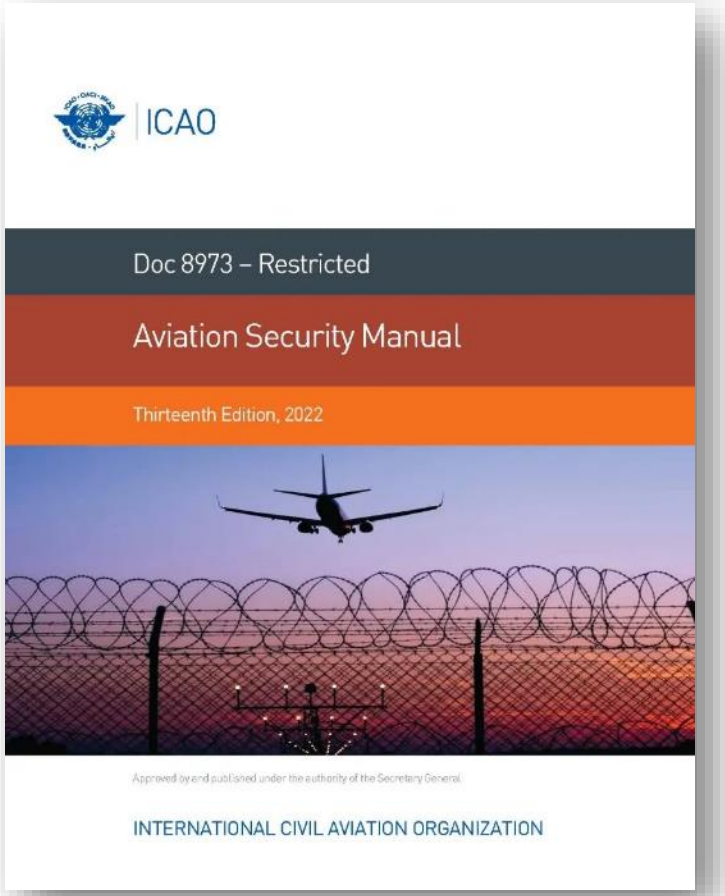
- PANS do not have the same status as the Standards and Recommended Practices.

- While the PANS may contain material which may eventually become SARPs when it has reached the maturity and stability necessary for adoption as such, they may also comprise material prepared as an amplification of the basic principles in the corresponding SARPs, and designed particularly to assist the user in the application of those SARPs.

- To qualify for PANS status, the procedure shall be agreed as suitable for application on a world-wide basis, although the need to apply it in a given area may be subject to regional agreement.

Guidance Material

Guidance Material provides guidance and information in amplification of the SARPs and PANS, the implementation of which they are designed to facilitate. They are often used to explain the objective of specific requirements and provide implementation examples, means of compliance, and/or best practices.



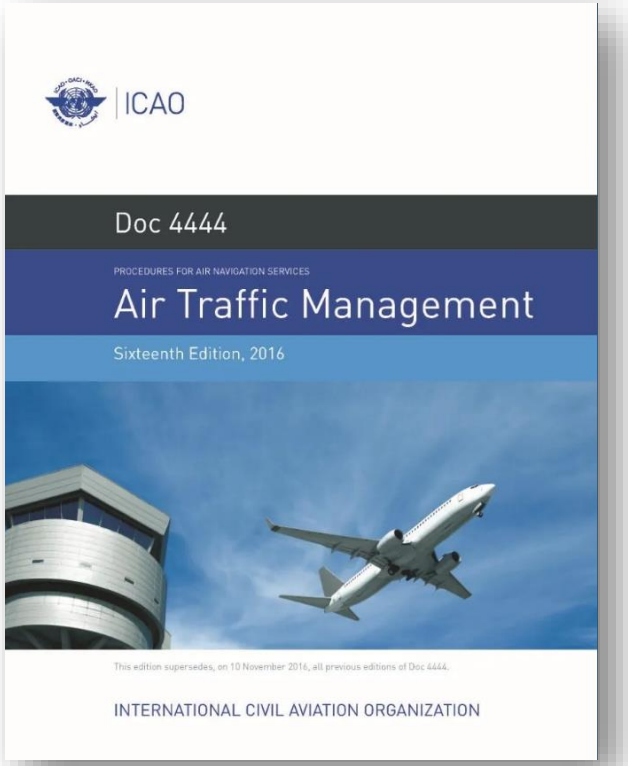
ICAO Publications

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

Why Cybersecurity in Civil Aviation?

Impact of Technology

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

However,
Inter-connection of digital systems between aviation stakeholders increases the cyber-threat surface to operational disciplines.

ICAO

Milestones of ICAO's Work on Aviation Cybersecurity

2005
Global Operational ATM concept

2014
IHLG - Civil Aviation Cybersecurity Action Plan
1st SARP in Annex 17

2016
A39-19

2017
Secretariat Study Group on Cybersecurity

2019
Aviation Cybersecurity Strategy – A 40-10
Trust Framework Study Group

Major Milestones

2020
Cybersecurity Action Plan – 1st Edition

2022
Cybersecurity Action Plan -2nd Edition

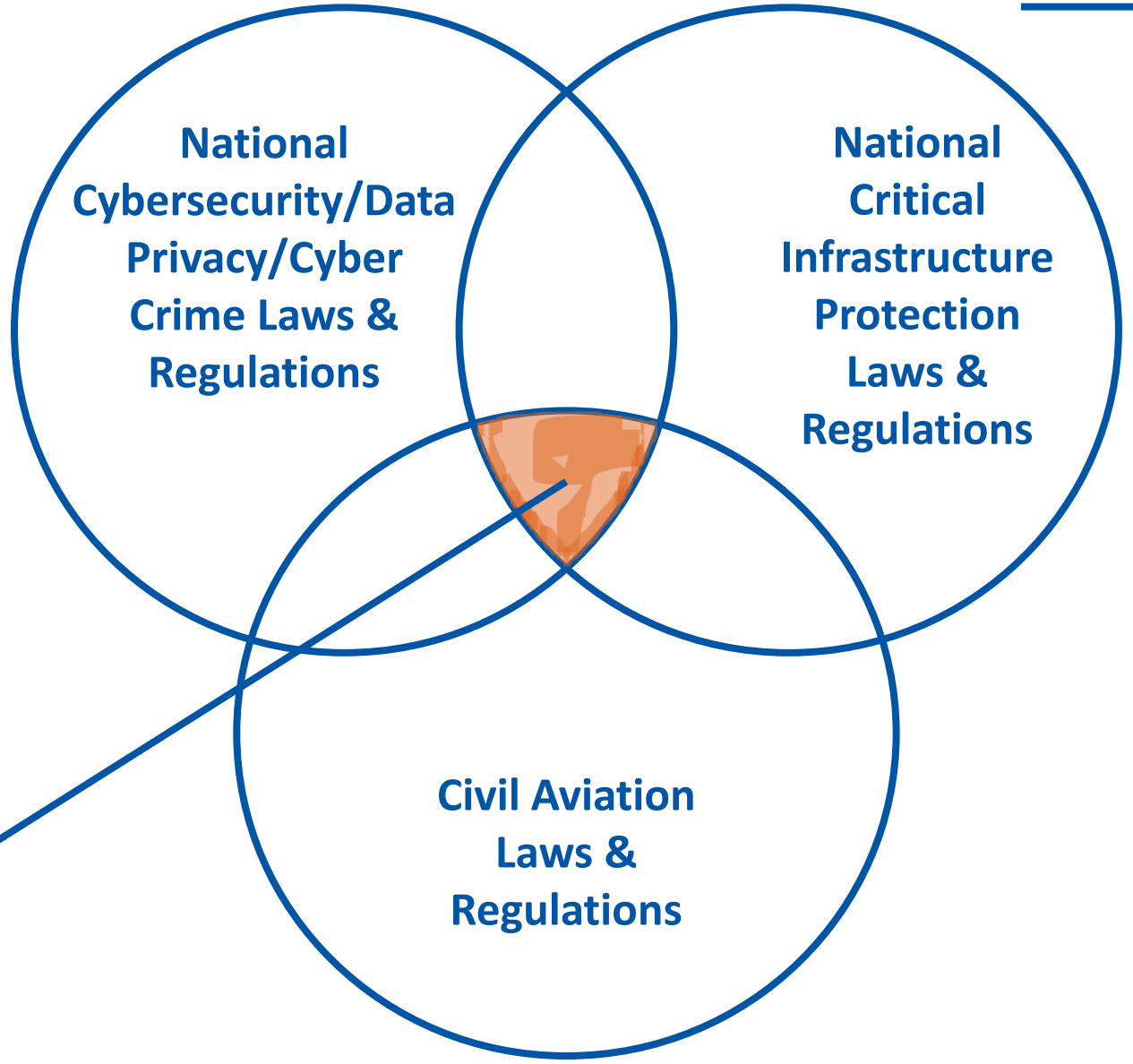
A 41-19: Establishment of:

- the Ad Hoc Cybersecurity Coordination Committee (AHCCC)
- Cybersecurity Panel (CYSECP)
- Trust Framework Panel (TFP)

Aviation Cybersecurity & the Role of ICAO

Efforts to address aviation cybersecurity should be:

- Consistent
- Clear
- Harmonized
- Trusted
- Cross-cutting across aviation disciplines
- In line with global priorities
- Coordinated with concerned stakeholders outside the Aviation Ecosystem



Definitions/What is Aviation Cybersecurity?

Cross-Sectoral

"The process of protecting information by preventing, detecting, and responding to attacks"

"The preservation of confidentiality, integrity and availability of information in the cyberspace"

Aviation

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

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 relevant 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 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.*

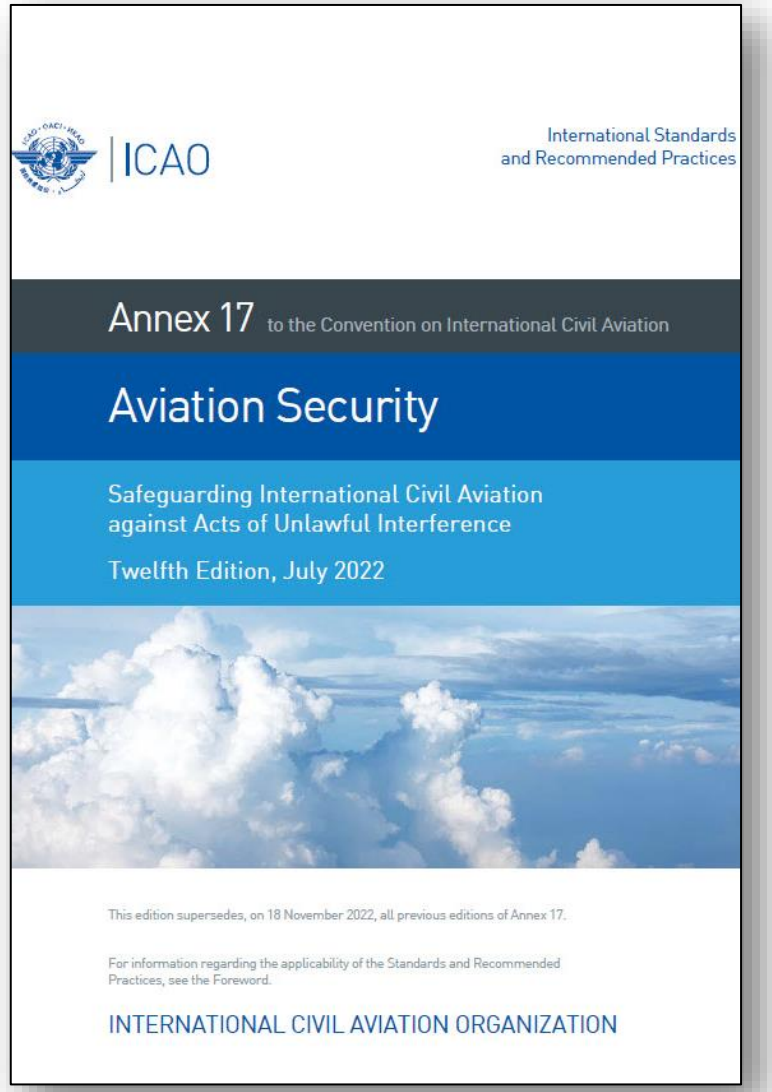
Definitions/Glossary of Terms

Confidentiality	*Property that an asset is not being made available or disclosed to unauthorized individual, user, programme, process, system or device.*
Integrity	*Property of accuracy and completeness of an asset, supporting what the asset claims to be.*
Availability	*Property of being accessible and usable upon demand by an authorized individual, user, programme, process, system or device.*
Cyber-attack	*The intentional use of electronic means to interrupt, alter, destroy, or gain unauthorized access to cyber assets.*
Attack Vector	*The means used to begin an attack.*
Threat Entity (or Actor)	*Entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization or system.*

ICAO Standard & Recommended Practice on Cybersecurity

Annex 17 to the Chicago Convention – Aviation *Security*

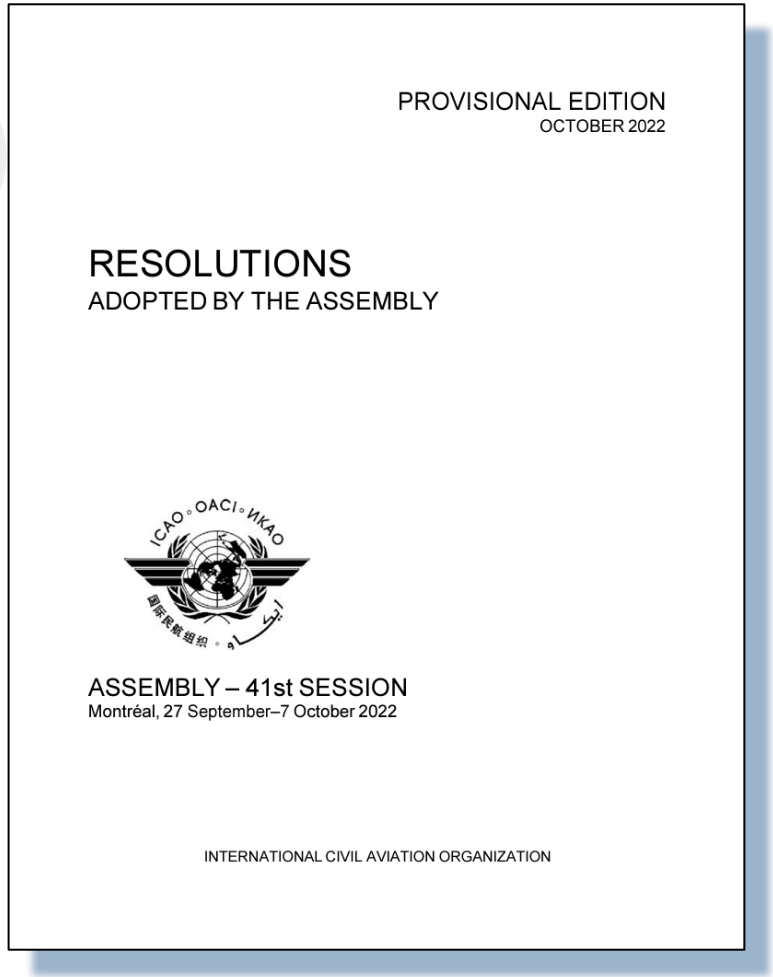
- **Standard 4.9.1**
  - Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation **identify** their critical information and communications technology systems and data used for civil aviation 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 Assembly Resolutions on Aviation Cybersecurity

A41–19: Addressing Cybersecurity in Civil Aviation

- **Global Adoption** — Beijing Instruments
- **Cooperation** — National, Regional and Global States and Industry
- **Implementation** — ICAO Strategy and Action Plan
- **Governance** — Define Responsabilities, Identify Competent Authority…
- **Others** — Risk management framework, cybersecurity culture …


PROVISIONAL EDITION
OCTOBER 2022

RESOLUTIONS
ADOPTED BY THE ASSEMBLY

ASSEMBLY – 41st SESSION
Montréal, 27 September–7 October 2022

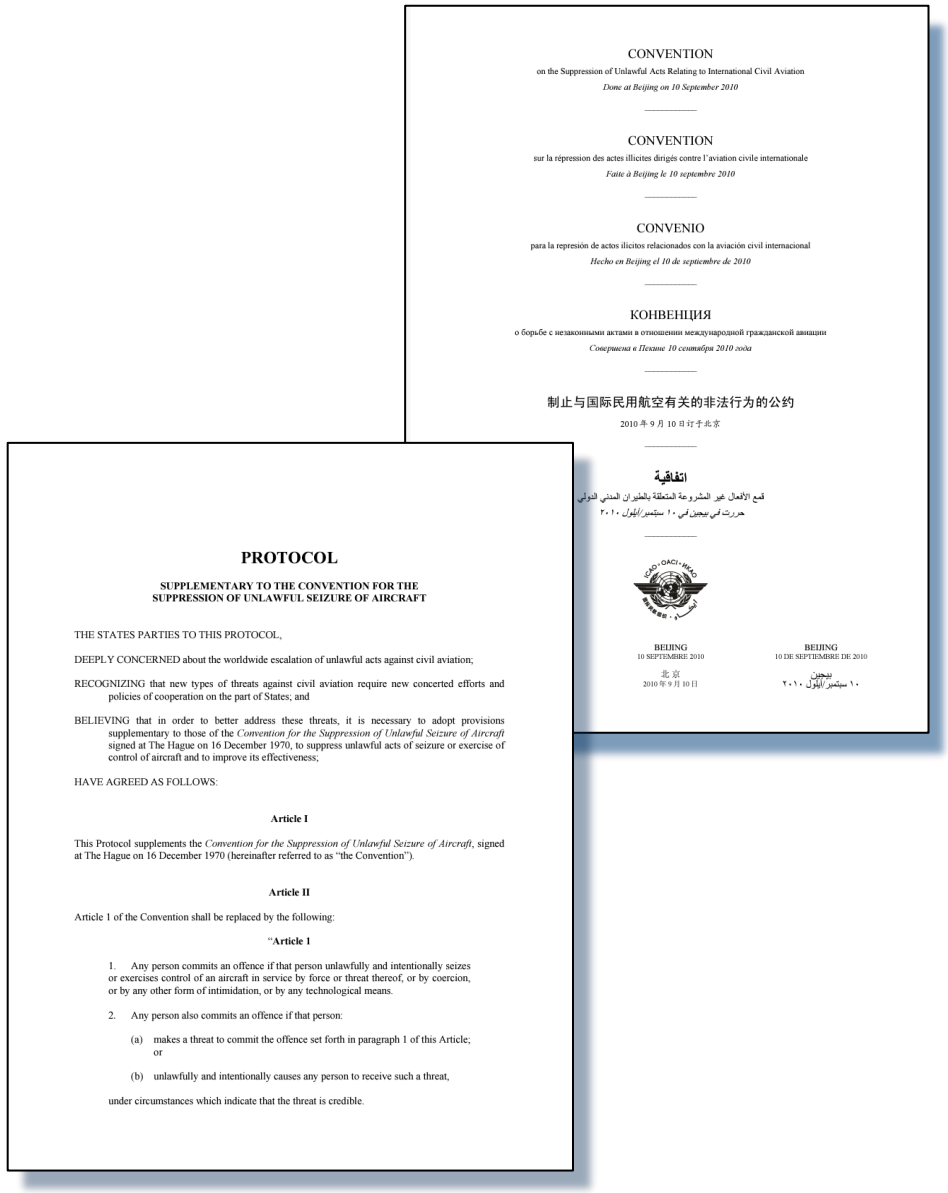
INTERNATIONAL CIVIL AVIATION ORGANIZATION

https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf

International Legal Instruments

- **The Beijing Convention (2010)** on the suppression of unlawful acts relating to International civil aviation
- **The Beijing Protocol (2010)** supplementary to the Hague Convention (1970) for the suppression of the unlawful seizure of aircraft

Governments' Adoption of the Beijing Instruments is an Important **DETERRENT of Cyber-Attacks** Against Civil Aviation



CONVENTION
on the Suppression of Unlawful Acts Relating to International Civil Aviation
Done at Beijing on 10 September 2010

CONVENTION
sur la répression des actes illicites dirigés contre l'aviation civile internationale
Faite à Beijing le 10 septembre 2010

CONVENIO
para la represión de actos ilícitos relacionados con la aviación civil internacional
Hecho en Beijing el 10 de septiembre de 2010

КОНВЕНЦИЯ
о борьбе с незаконными актами в отношении международной гражданской авиации
Совершена в Пекине 10 сентября 2010 года

制止与国际民用航空有关的非法行为的公约
2010 年 9 月 10 日订于北京

اتفاقية
لقمع الأفعال غير المشروعة المتعلقة بالطيران المدني الدولي
حررت في بيجين في ١٠ سبتمبر/أيلول ٢٠١٠

BEIJING
10 SEPTEMBRE 2010

BEIJING
10 DE SEPTIEMBRE DE 2010

北京
2010 年 9 月 10 日

بيجين
١٠ سبتمبر/أيلول ٢٠١٠

PROTOCOL

SUPPLEMENTARY TO THE CONVENTION FOR THE SUPPRESSION OF UNLAWFUL SEIZURE OF AIRCRAFT

THE STATES PARTIES TO THIS PROTOCOL,

DEEPLY CONCERNED about the worldwide escalation of unlawful acts against civil aviation;

RECOGNIZING that new types of threats against civil aviation require new concerted efforts and policies of cooperation on the part of States; and

BELIEVING that in order to better address these threats, it is necessary to adopt provisions supplementary to those of the *Convention for the Suppression of Unlawful Seizure of Aircraft* signed at The Hague on 16 December 1970, to suppress unlawful acts of seizure or exercise of control of aircraft and to improve its effectiveness;

HAVE AGREED AS FOLLOWS:

Article I

This Protocol supplements the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on 16 December 1970 (hereinafter referred to as "the Convention").

Article II

Article 1 of the Convention shall be replaced by the following:

"**Article 1**

1. Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means.

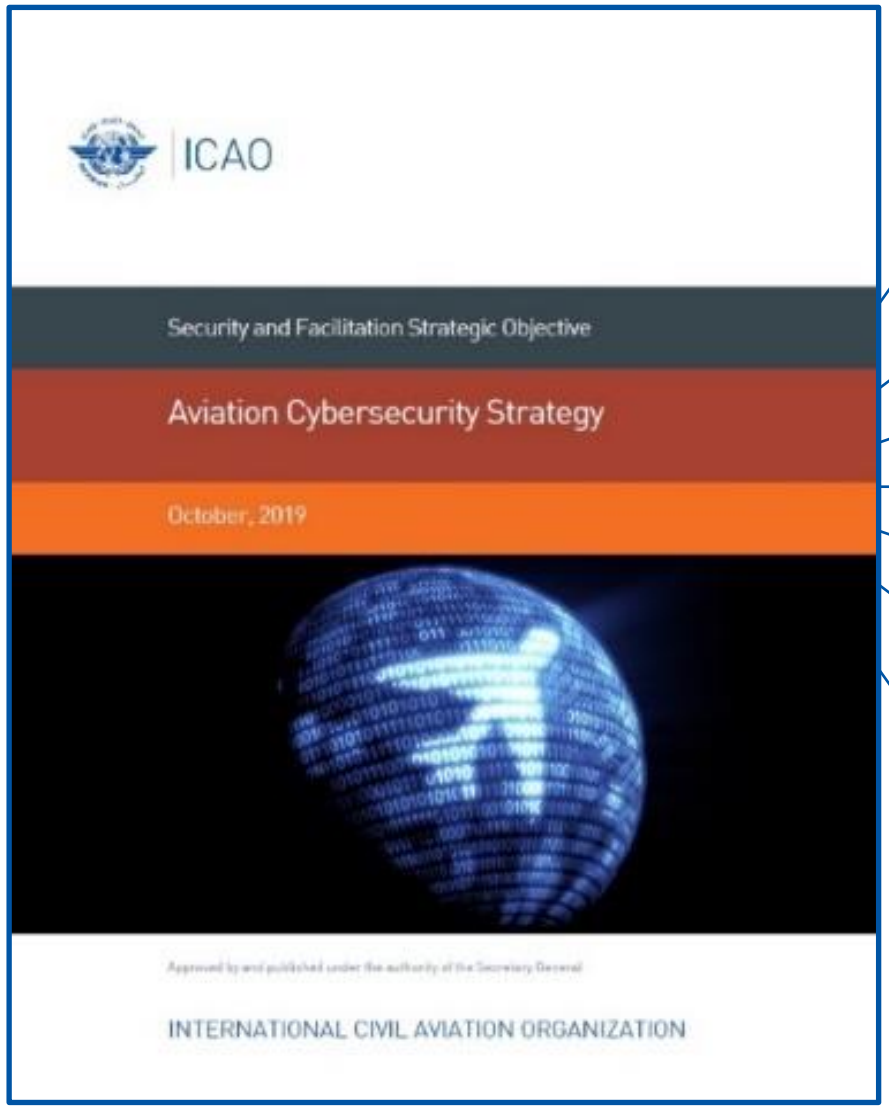
2. Any person also commits an offence if that person:

(a) makes a threat to commit the offence set forth in paragraph 1 of this Article; or

(b) unlawfully and intentionally causes any person to receive such a threat,

under circumstances which indicate that the threat is credible.

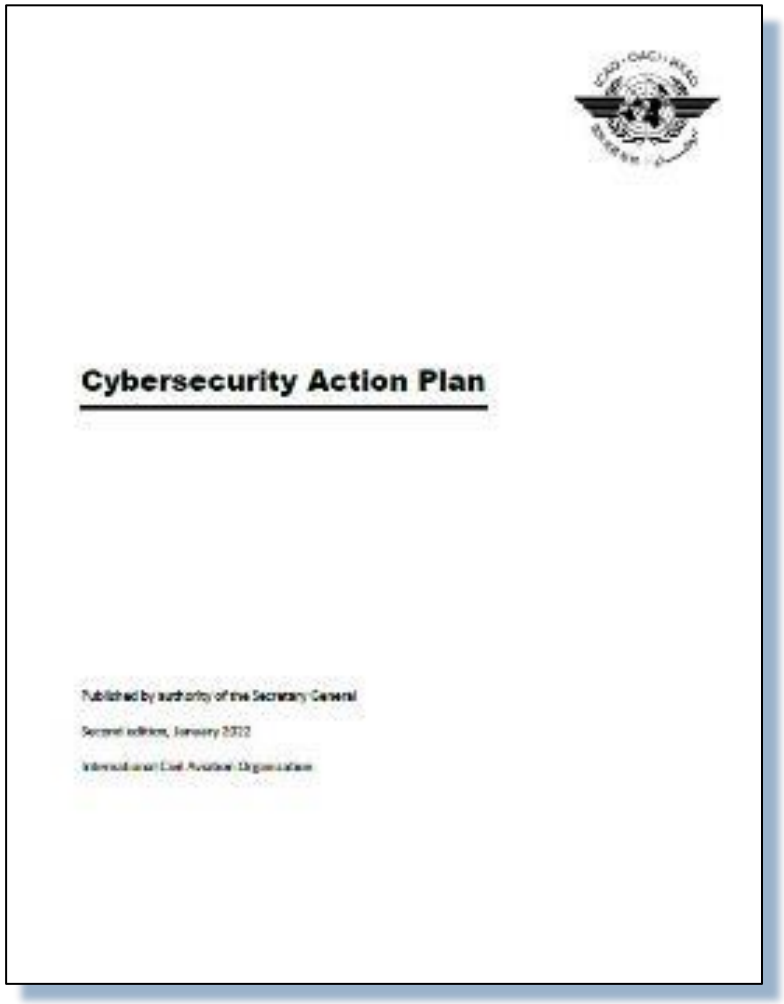
ICAO Aviation Cybersecurity Strategy



- 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

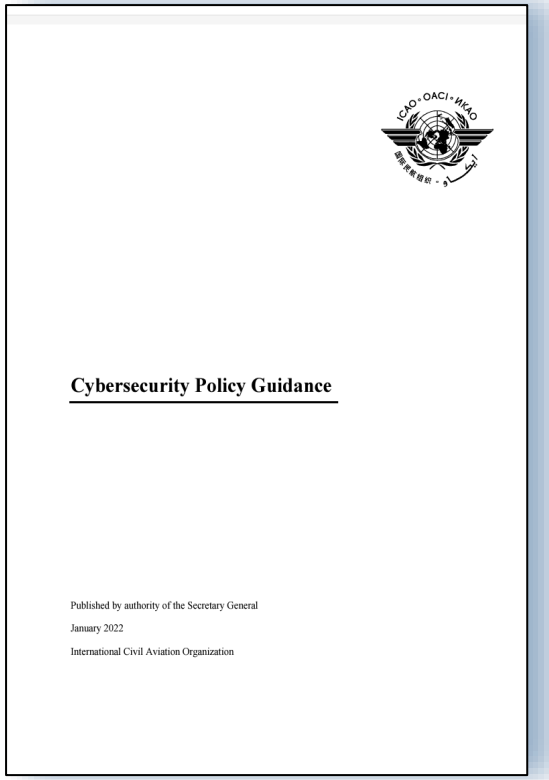
Develops the **7 Pillars** of the Aviation Cybersecurity Strategy into **32 Priority Actions**, which are further broken down into **51 Tasks** to be implemented by ICAO, States, and Stakeholders

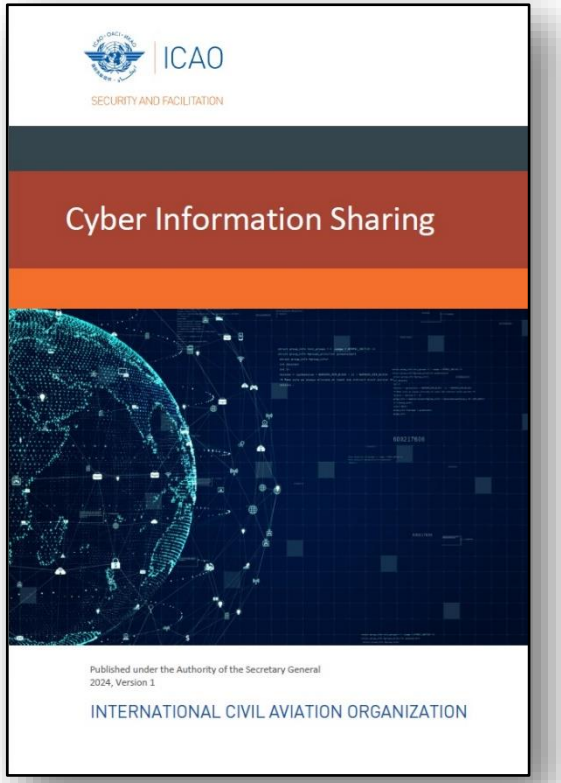
https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

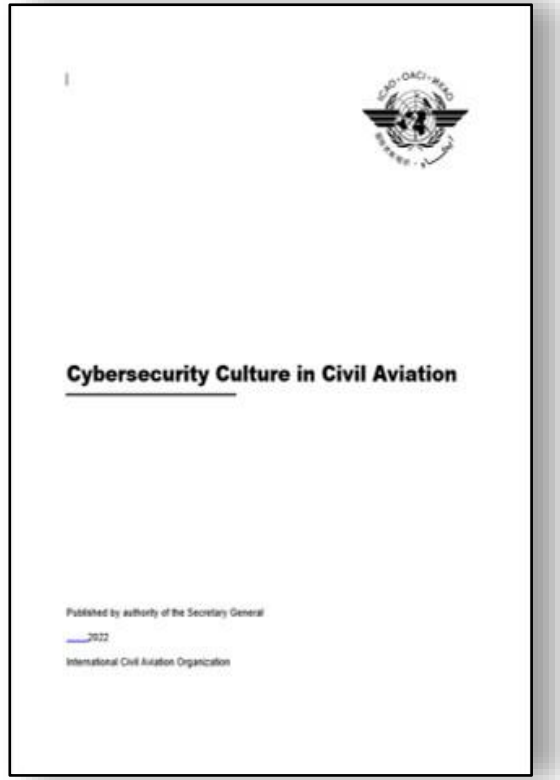
Cybersecurity Action Plan (Example)

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

Aviation Cybersecurity Guidance Material



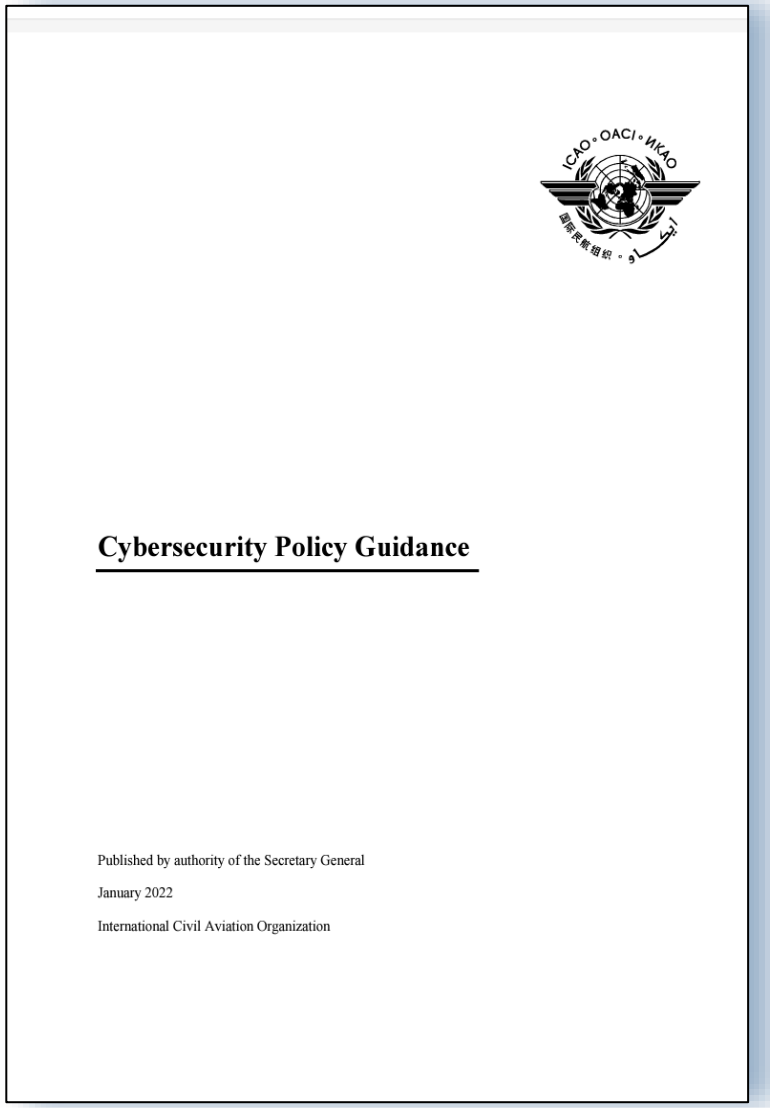




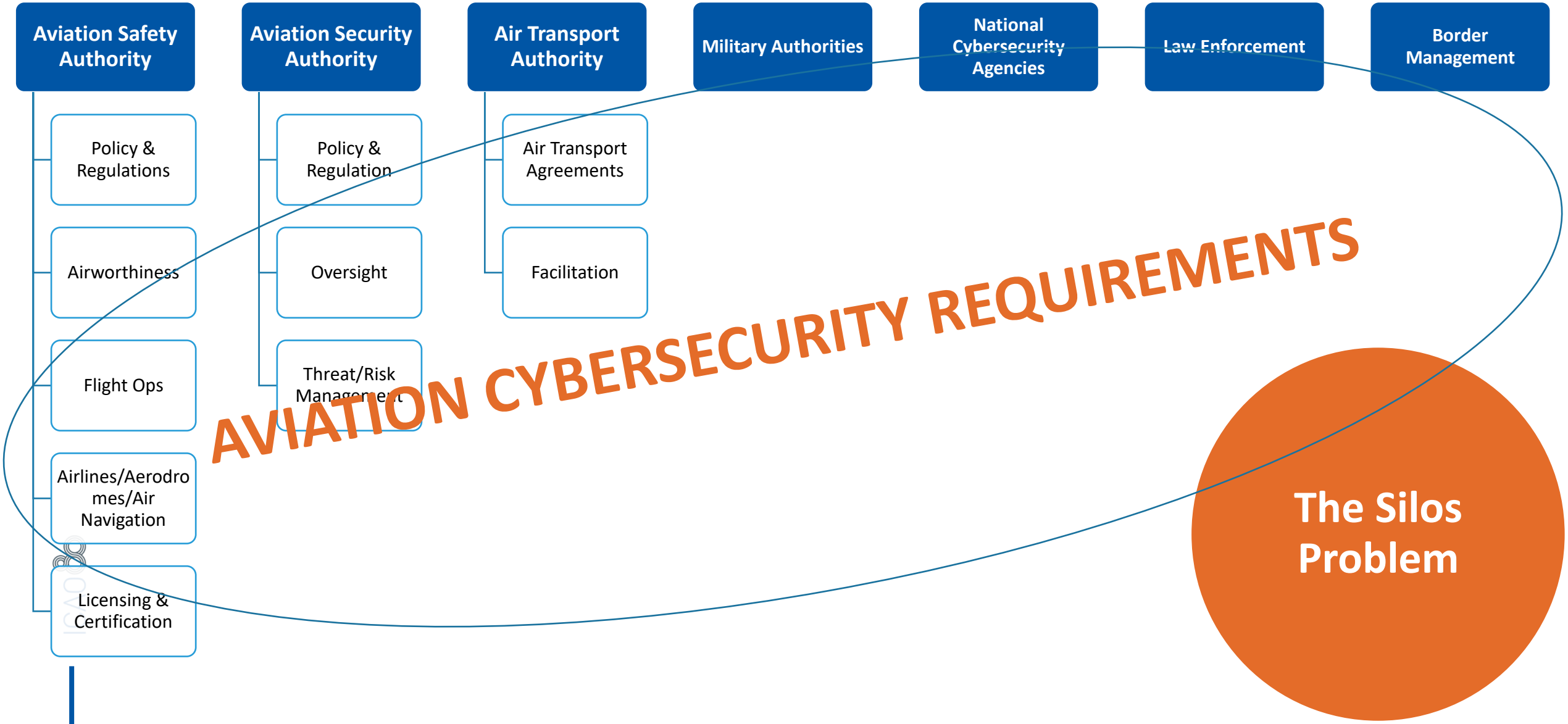
https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

Aviation Cybersecurity Guidance Material

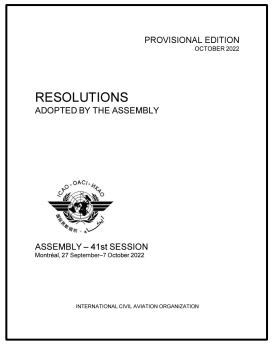
"What if we don't change at all ...
and something magical just happens?"



Aviation Cybersecurity Governance

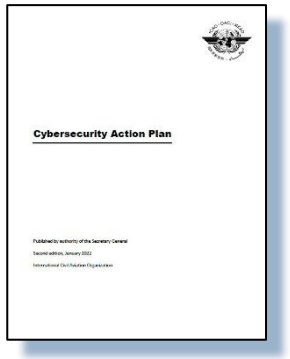


Aviation Cybersecurity Governance



- **Assembly Resolution A41–19:** calls upon States to:
  - designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies.
  - define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation.

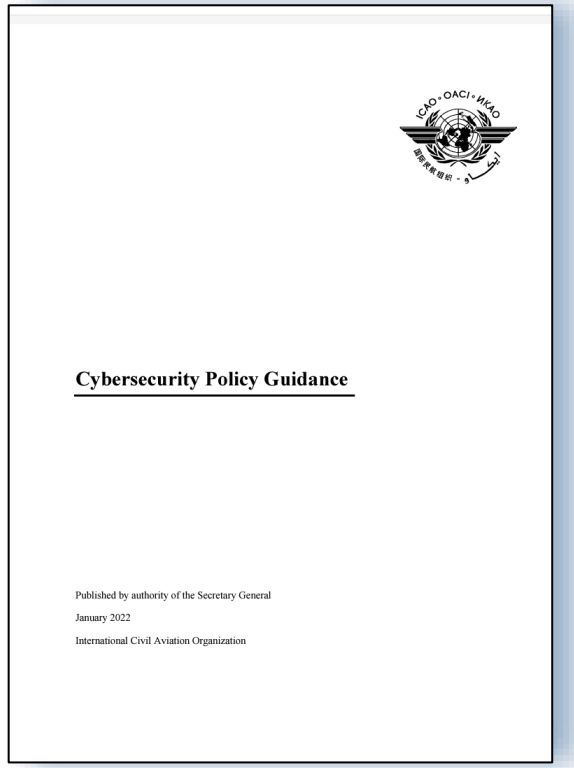
- **ICAO Aviation Cybersecurity Strategy:** Pillar 2 – Governance:
  - States are encouraged to develop clear national governance and accountability for civil aviation cybersecurity. Civil Aviation authorities are encouraged to ensure coordination with their competent national authority for cybersecurity, recognizing that the overall cybersecurity authority for all sectors may reside outside the responsibility of the civil aviation authority. It is also essential that appropriate coordination channels among various State authorities and industry stakeholders be established.



- **Cybersecurity Action Plan:**
  - Cybersecurity governance should be policy-driven and enforced, and accountability needs to be determined for compliance.

ICAO 80

Aviation Cybersecurity Governance

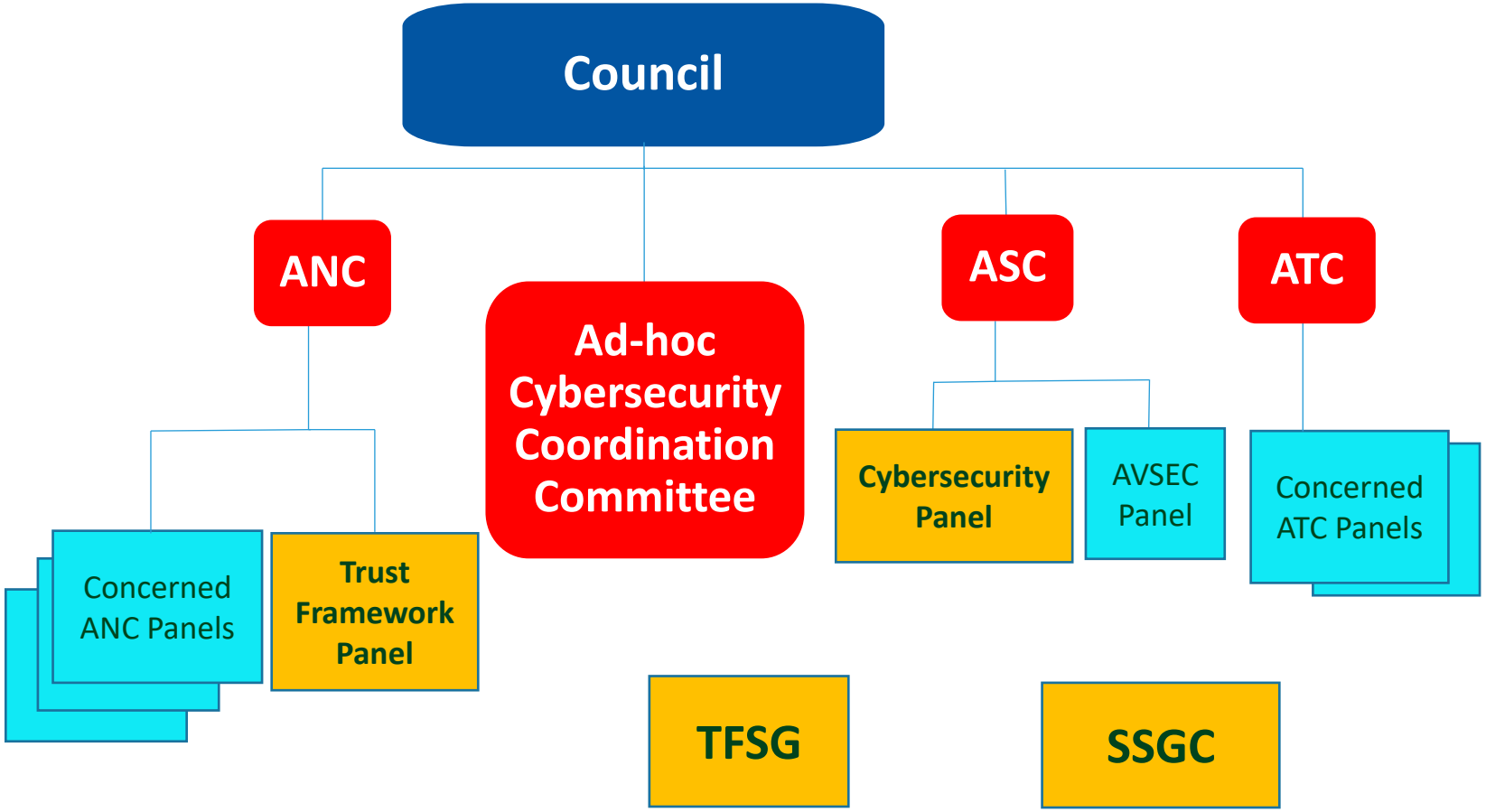


- States should designate an Appropriate Authority for Aviation Cybersecurity (AA/Cyber) with an overall mandate and responsibility for aviation cybersecurity.

The Appropriate Authority for Aviation Cybersecurity should:

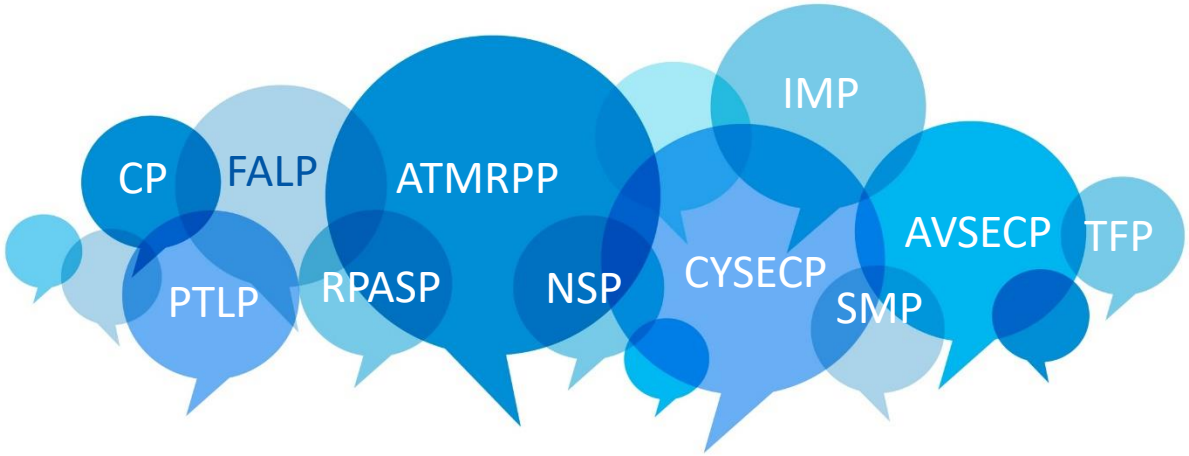
- determine, in coordination with the national competent authority for cybersecurity, the roles and responsibilities to be undertaken by each authority;
- lead the development of aviation cybersecurity regulations;
- clearly define roles and responsibilities for the different civil aviation domains within the national competent authority for civil aviation;
- coordinate the definition of roles and responsibilities of civil aviation entities overseen by the national competent authority for civil aviation through the national safety and security programmes;
- define the elements of civil aviation cybersecurity culture and monitor its implementation;
- define regulations, processes, requirements, and roles for cybersecurity crisis management, including testing requirements and frequencies; and
- coordinate cross-cutting aviation cybersecurity issues with relevant non-aviation stakeholders involved in aviation cybersecurity such as information sharing and incident investigation.

Aviation Cybersecurity Governance – ICAO Example



ICAO Council's Ad-Hoc Cybersecurity Coordination Committee (AHCCC)

- One Member of Each of the Council's Aviation Security Committee (ASC), Air Transport Committee (ATC).
- One Member from the Air Navigation Commission (ANC).
- One Member of Each ICAO Expert Group Regularly Addressing cybersecurity in its Work Programme (ATMRPP, AVSECP, CP, CYSECP, FALP, IMP, NSP, PTLP, RPASP, SMP, TFP)



Aviation Cybersecurity Policy Model

Model Cybersecurity Policy

1. **Introduction**
   - This cybersecurity policy shall be the framework for further development and implementation of aviation cybersecurity. It shall be published, disseminated to relevant stakeholders, and periodically reviewed.
   - Further guidance material shall be developed to support the implementation of this cybersecurity policy.

2. **Scope**
   - Aviation cybersecurity shall address the security and resilience of the civil aviation system, as well as support the collaboration with concerned non-aviation entities and authorities, including national cybersecurity authority, national security, law enforcement and military, as appropriate.
   - Aviation cybersecurity shall be coordinated at the national level with aviation safety, aviation security, critical infrastructure protection, cyber defence and military.
   - Aviation cybersecurity shall be coordinated at the international level with equivalent Foreign Appropriate Authorities designated for Aviation cybersecurity.

3. **Objectives**
   - The overall objectives of this aviation cybersecurity policy are to ensure the security, resilience, and self-strengthening of the civil aviation system against cyber threats and risks, and to ensure the coordination of aviation cybersecurity with concerned national authorities and entities.

3. **Governance and Organization**
   - In accordance with [Regulation/Legislation Reference for the designation], [Entity Name] shall be the Appropriate Authority for Aviation Cybersecurity (AA/Cyber) with an overall mandate for aviation cybersecurity and cyber resilience.
   - The AA/Cyber shall:
     - engage with the national competent authority for cybersecurity in order to define the civil aviation cybersecurity roles and responsibilities to be undertaken by each authority;
     - coordinate and contribute to the development of aviation cybersecurity regulations;
     - define, coordinate, and provide support to aviation safety and aviation security appropriate authorities to include aviation cybersecurity requirements, including oversight and quality control elements, in the national State Safety Programme (SSP) and the National Civil Aviation Security Programme (NCASP);
     - define, support, and monitor the implementation of the cybersecurity culture programme by all civil aviation stakeholders;
     - define regulations, processes, requirements, and roles for cybersecurity crisis management; and
     - coordinate cross-cutting aviation cybersecurity issues with relevant non-aviation stakeholders involved in aviation cybersecurity.

4. **Risk Management**
   - Cybersecurity shall be intelligence driven, threat based and risk managed.
   - Risk management shall be an integral part of overall systems' life cycle.
   - All data and systems shall have identified ownership at all times.

5. **Critical Systems Security**
   - Critical functions, systems, and infrastructure shall be identified through risk management processes.
   - Security by design approach, coupled with Defence in depth principles, shall be applied to protect critical systems.
   - Redundancy of critical systems shall be considered as an enabler for system security.

6. **Data Security**
   - Data and information shall be protected during storage and transmission, in line with its sensitivity profile.

7. **Supply Chain Security**
   - End-to-end management of software/hardware supply chain shall be part of aviation cybersecurity management.
   - Software and hardware used in critical aviation functions shall comply with cybersecurity requirements throughout the life cycle of aviation systems.

Aviation Cybersecurity Policy Model

8. **Physical Security**
   - Physical security (including personnel security) shall be part of aviation cybersecurity management.
   - Physical security shall safeguard people, infrastructure, facilities, equipment, material, and documents from unlawful interference and protect critical aviation systems from unauthorized physical access.
   - Physical security shall contribute to risk management through supporting the identification of threat actors and/or the likelihood of attacks on civil aviation critical infrastructure.

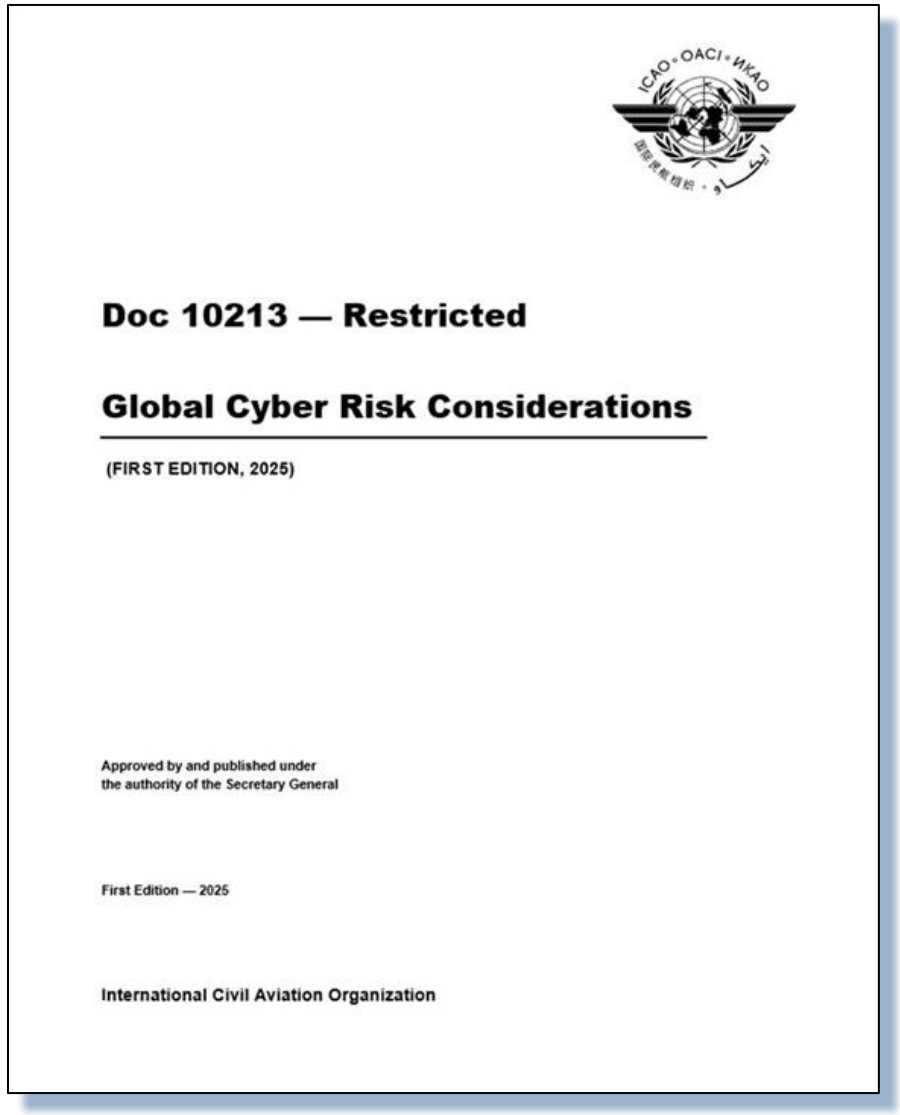
9. **Information, Communication, Technology (ICT) Security**
   - ICT security shall be part of aviation cybersecurity management.
   - ICT security shall define and implement logical security measures as well as contribute to cyber incident management, recovery, and operation continuity processes.
   - ICT security shall contribute to risk management through the identification of vulnerabilities, attack vectors, and monitoring the evolution of the aviation cybersecurity threat landscape.

10. **Incident Management and Continuity of Critical Functions**
    - Safety of operations and continuity of critical functions shall be the main drivers in incident management processes.
    - Testing crisis management and recovery plans shall be an integral part of incident management.

11. **Cybersecurity Culture**
    - An education, awareness, training, and exercise plan shall be an integral part of aviation cybersecurity management.
    - Cybersecurity culture shall be fully coordinated with existing safety and security cultures.
    - Cybersecurity culture shall be supported by robust internal and, to the extent possible, external information sharing practices.

Aviation Cyber Risk Management

"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."



Doc 10213 — Restricted

Global Cyber Risk Considerations

(FIRST EDITION, 2025)

Approved by and published under
the authority of the Secretary General

First Edition — 2025

International Civil Aviation Organization

Cyber Risk Management

Risk Management General Principles

1 Context Establishment

Understand the organizational environment, identify critical assets, and determine the threat landscape. Define the scope of risk management, risk tolerance, and key objectives.

2 Risk Identification

Identify potential threats and vulnerabilities through assessments of infrastructure, stakeholder interviews, and review of historical cyber incidents or current cyber threat intelligence.

3 Risk Analysis

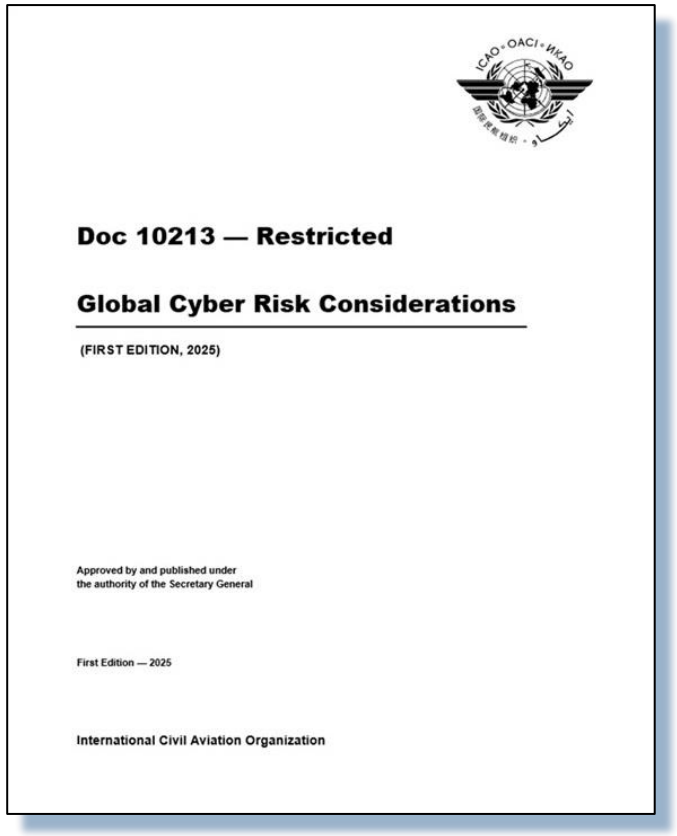
Analyze identified risks in terms of likelihood and impact, using qualitative or quantitative methods to understand the severity of each risk.

4 Risk Evaluation

Compare identified risks against established risk tolerance thresholds to prioritize which risks require immediate attention.

Cyber Risk Management

ICAO Global Cyber Risk Considerations – Doc 10213



Methodology to Integrate Cyber Risk Management into Aviation Risk Management

Global Cyber Threat & Risk Landscape

Cyber Risk Management

Integrating Cyber Risk Management into Aviation Safety, Security, Efficiency & Capacity Risk Management Processes

- ✓ Supports Protection & Resilience of Aviation Critical Infrastructure.
- ✓ Holistic Approach to risk management in aviation disciplines that consider cyber risk management as integral aspect of operations.
- ✓ Ensures Cyber risks are included in organizational strategic decision making process.

Integration Methodology

Step 0: Identify Critical Systems, data and information.

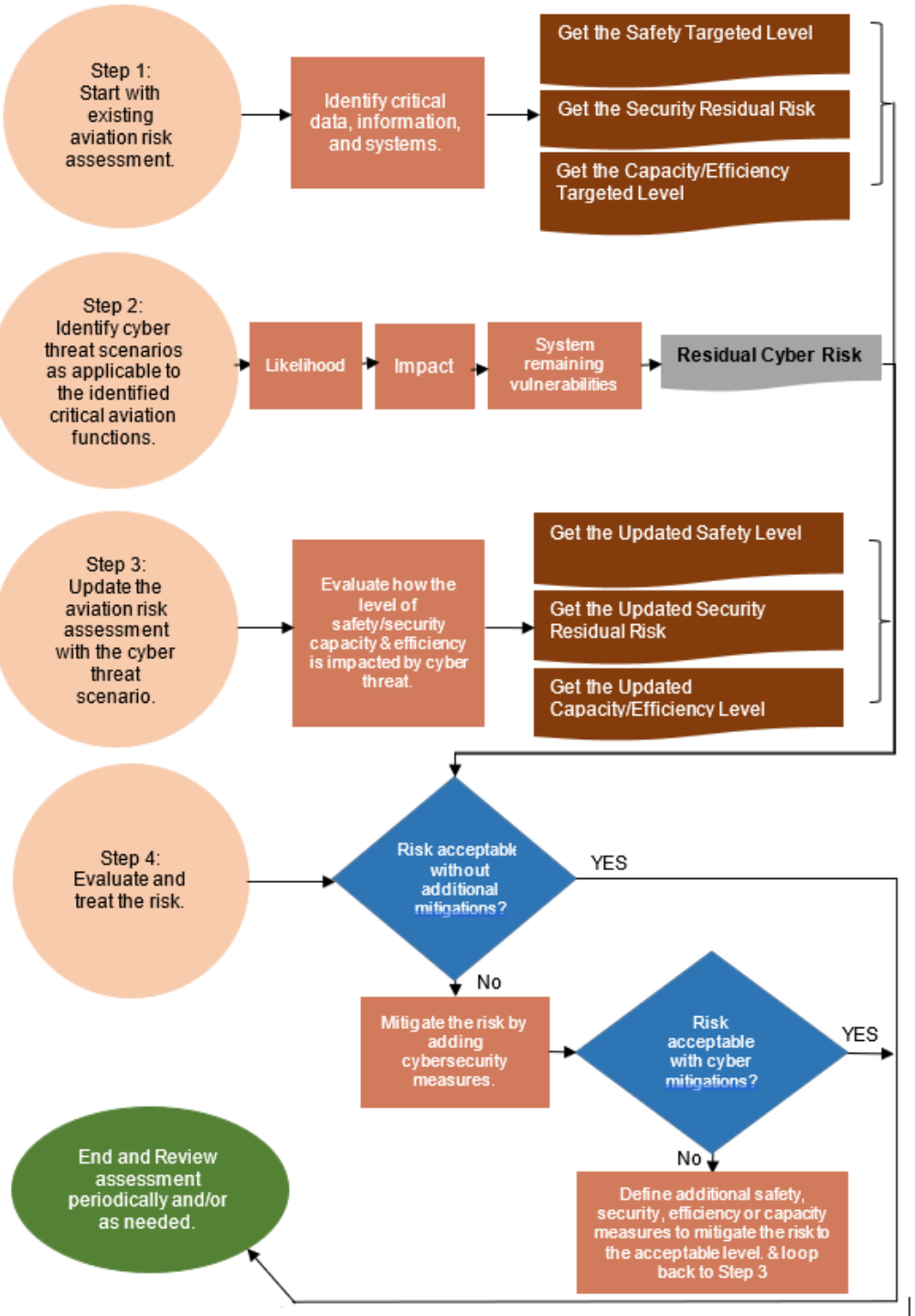
Step 1: Begin with Existing Aviation Risk Assessment.

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

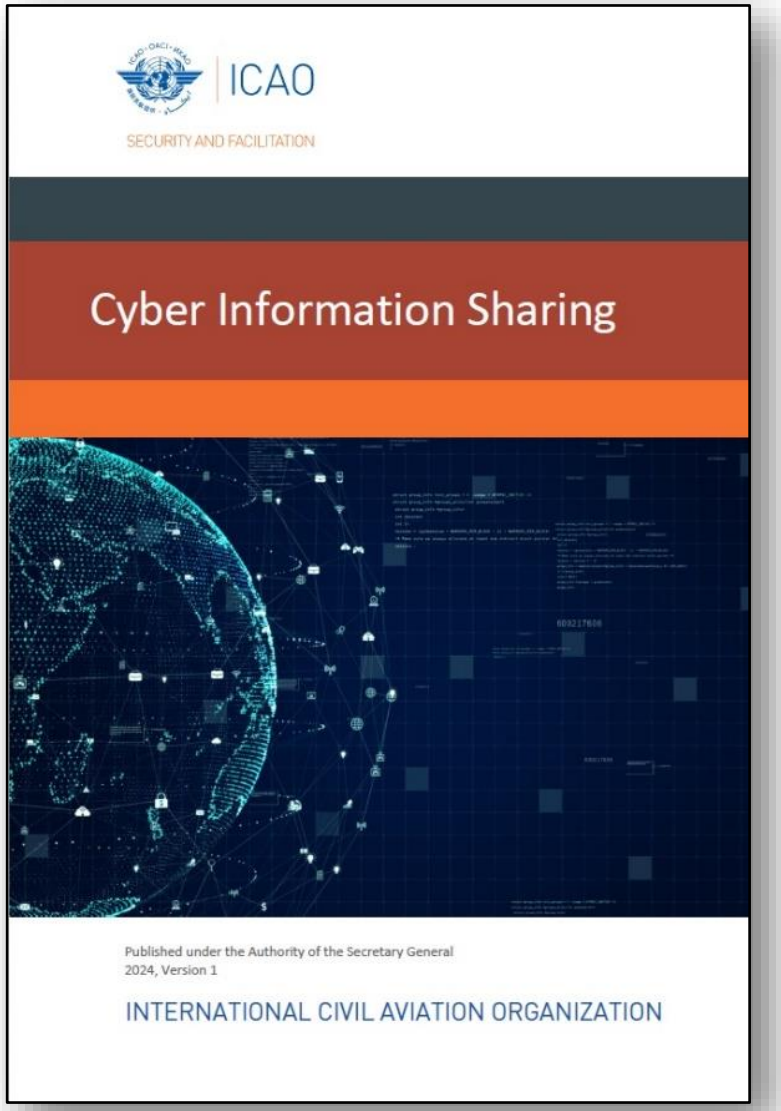
Step 3: Update Aviation Risk Assessment to Include Cyber Risk Assessment.

Step 4: Evaluate and Mitigate.

Step 5: Monitor and Review



Cyber Information Sharing



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

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

Steps to Develop and Implement 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. Enable Implementation: Scope sources and tools, maintain a POC, test systems, launch, and continuously improve.

Communication Tools that Can be Used

Important Considerations for Cyber Information Sharing

ASSESS TRUSTWORTHINESS AND RELIABILITY OF THE SOURCE

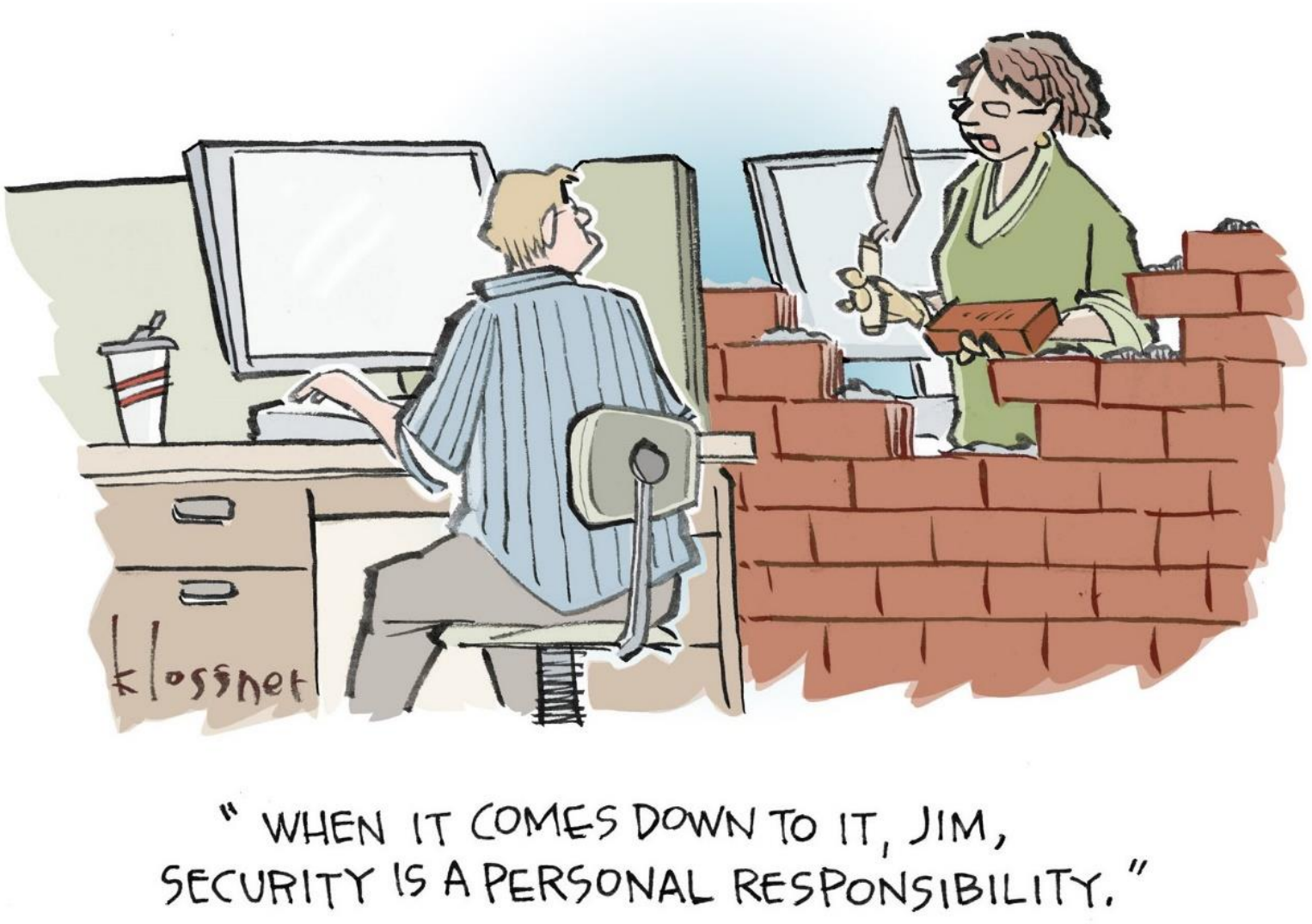
ANALYZE PLAUSIBILITY/CREDIBILITY OF THE INFORMATION

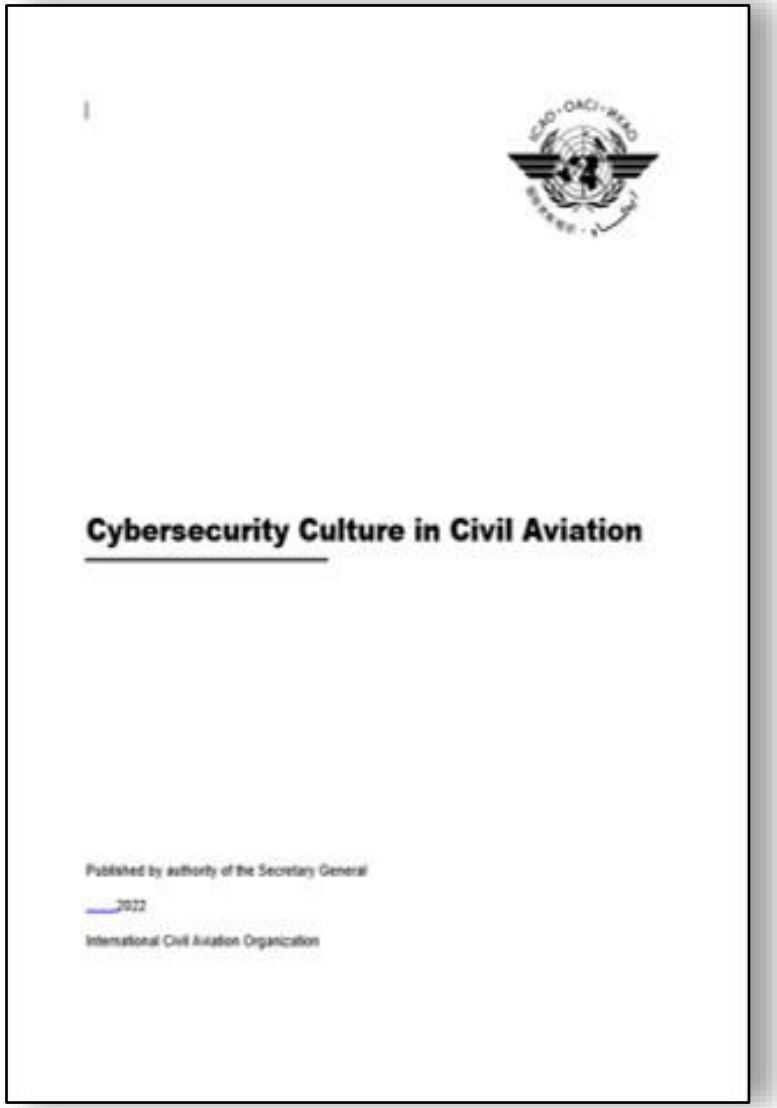
ANALYZE RELEVANCE TO ORGANIZATION, INFORMATION SHARING COMMUNITY, AND AVIATION ECOSYSTEM

Cyber Information Sharing: Traffic Light Protocol (TLP)

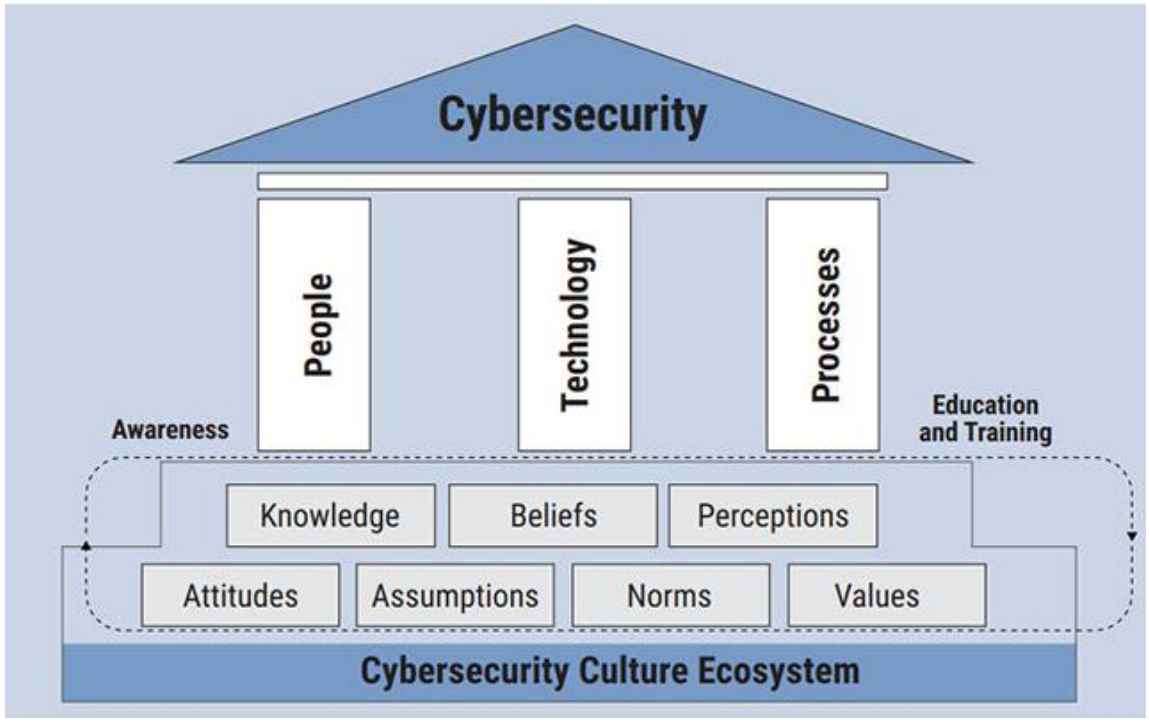
TLP:CLEAR	marking does not constraint the dissemination of the received information to anyone through any medium.
TLP:GREEN	Information can be shared within the aviation community.
TLP:AMBER	Information can be shared on a need-to-know basis within the organization of the recipient and its clients.
TLP:AMBER +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.

Cybersecurity Culture in Civil Aviation





Cybersecurity Culture in Civil Aviation



A set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the **daily operation of an organization** and are reflected by the actions and behaviours of all entities and personnel in their interaction with digital assets.

It aims to make cybersecurity considerations **part of the organization's habits, conducts, and processes**, by embedding them in daily operations as reflected by the actions and behaviours of all personnel.

Cybersecurity Culture in Civil Aviation

Benefits of a Robust Cybersecurity Culture:

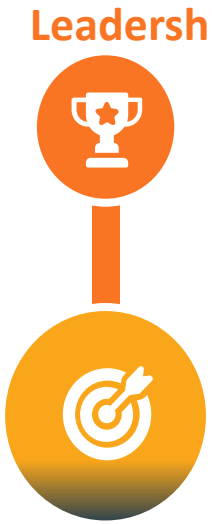
- Enhanced cybersecurity maturity of the organization.
- Appropriate handling of information by everyone.
- improved cybersecurity posture.
- enhanced awareness to cyber risks.
- willingness to report.

Building a Cybersecurity Culture

SAFETY CULTURE

SECURITY CULTURE

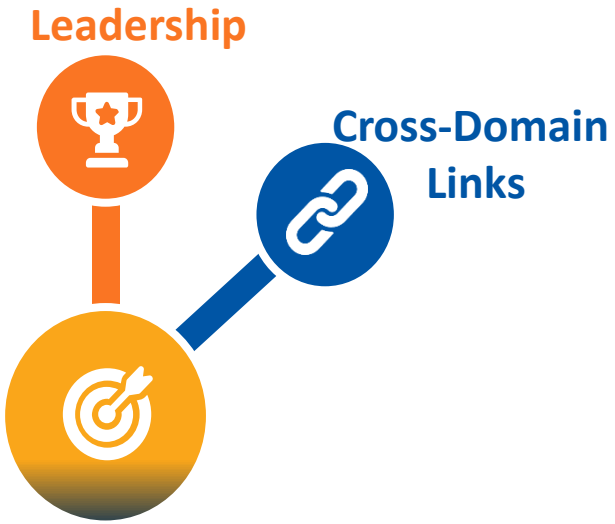
Core Elements: Leadership



Senior Management:

- ✓ Commit to Cybersecurity Culture
- ✓ Ensure appropriate resources are allocated
- ✓ Lead by Example and abide by rules and processes
- ✓ Make cybersecurity an organizational priority
- ✓ Support implementation, awareness, training, and capacity building
- ✓ Follow up on report processing and resolution
- ✓ Intervene when needed
- ✓ Monitor the cyber posture of the organization

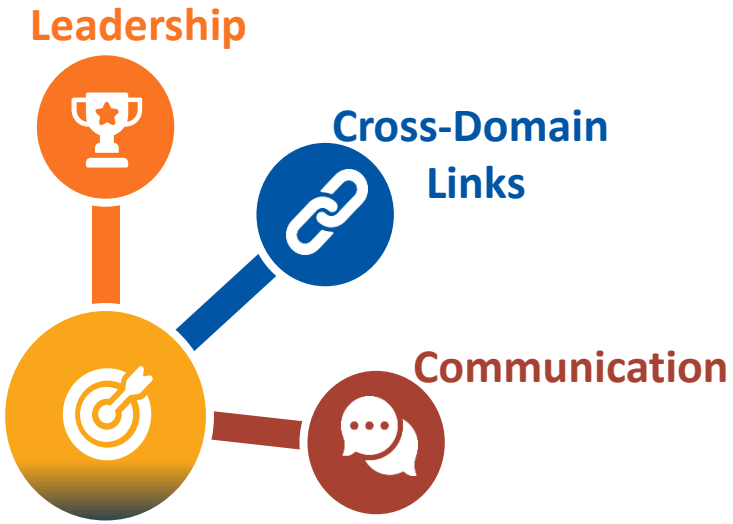
Core Elements: Cross-Domain Links



Multidisciplinary Task Force:

- ✓ Assess maturity of culture
- ✓ Identify risks and opportunities in culture implementation
- ✓ Bridge requirements of internal stakeholders
- ✓ Support cross-domain activities to foster organizational culture

Core Elements: Communication



Elements:

- ✓ Communication Skills (style, clarity, listening)
- ✓ Downstream explanation of policies and guidelines

Supports:

- ✓ Awareness
- ✓ Compliance

Core Elements: Awareness, Training, Education

Core Elements: Reporting Systems

Contains elements aimed to:

- ✓ ensure confidentiality of personal information
- ✓ define clear policy on confidentiality of handling collected information
- ✓ provide adequate training to all personnel on using the reporting system
- ✓ provide awareness on and implement “just culture” in cybersecurity reporting
- ✓ Implement incentive programme to encouraging personnel to report their own errors as well as any suspicious cyber behaviours they observe

Core Elements: Continuous Review & Improvement

Developing Performance Indicators including:

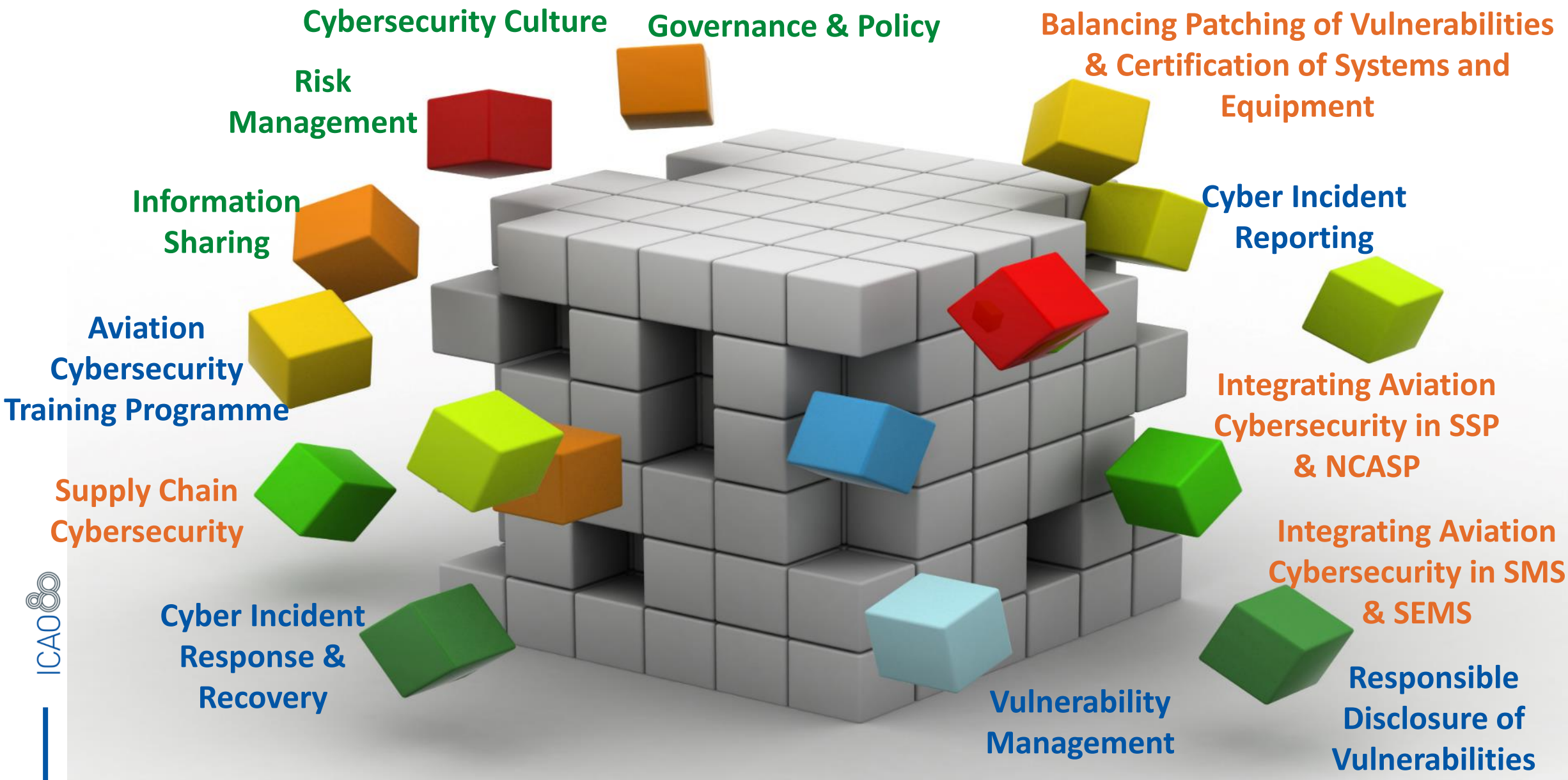
- ✓ Statistics on reports/compare with organization's logs
- ✓ Results of recurrent training
- ✓ Results of tests/simulations of cyber incidents
- ✓ Questionnaires/interviews/etc.

Core Elements: Positive Work Environment

Elements:

- ✓ Setting targets on cyber incidents to and periodic briefings on achievements
- ✓ Provision of adequate procedures, training, and tools to personnel
- ✓ Involvement of personnel in decision-making/feedback
- ✓ Allocate time for training
- ✓ Recognize good performance
- ✓ Timely response to feedback and reports
- ✓ Providing personnel with appropriate levels of responsibility

Guidance Material in the Pipeline



Guidance Material in the Pipeline – Aviation Cybersecurity Manual

- Introduction / Executive Summary / Scope / Acronyms
- Glossary of Terms
- State Policy & Regulatory Aspects:
  - Aviation Cybersecurity Governance
  - Aviation Cybersecurity Policy
  - Principles for Integrating aviation cybersecurity into the State Safety Program (SSP)/National Civil Aviation Security Program (NCASP)
  - National/International Legal framework
  - Oversight Functions
- Integrating aviation cybersecurity into SMS, SEMS and ISMS
- Cyber Risk Management
- Cybersecurity Culture
- Personnel Security
- Insider Threat
- Physical Security
- Cyber Information Sharing
- Cyber Incident Reporting
- Cyber Supply Chain Management
- Cyber Incident Response & Recovery / Emergency Response Planning
- Vulnerability Management Programme
- Balancing Patching Vulnerabilities and certification requirements
- Responsible Disclosure of Vulnerabilities
- Continuous Improvement
- Aviation Cybersecurity Training Programme
- Quality Management
- Appendices

Available ICAO Capacity Building Resources

- Foundations of Aviation Cybersecurity Leadership and Technical Management (with Embry-Riddle Aeronautical University).

https://www.enrole.com/erau/jsp/course.jsp?categoryId=5586BD00&courseId=SGC-1102

- Aviation Cybersecurity Oversight (with UK CAAi)

https://caainternational.com/course/icao-aviation-cybersecurity-oversight/

Thank You

ICAO 80