ICAO

RECONNECTINGTHEWORLD

Global Developments in Aviation Cybersecurity

Rashad Karaky
Aviation Cybersecurity Officer
International Civil Aviation Organization

ICAO

RECONNECTINGTHEWORLD

Agenda

- What is ICAO?
- Why Cybersecurity in Civil Aviation?
- ICAO's Work on Aviation Cybersecurity & Cyber Resilience
- The Aviation Cybersecurity Strategy and Action Plan
- Cybersecurity Guidance Material
- International Aviation Trust Framework
- Training & Capacity Building Initiatives

ICAO

RECONNECTINGTHEWORLD

ICAO - International Civil Aviation Organization

- **UN Specialized Agency** established in 1947 (Chicago Convention 1944)
- **193** Member States
- Assembly, Council, Commission, Committees supported by the Secretariat
- Issuing Conventions, Protocols, Resolutions, Standards and Recommended Practices (SARPS) addressed to States
- Auditing of States
- Providing assistance, training and capacity building to States

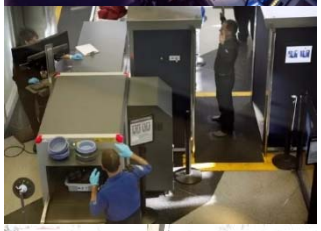
ICAO

RECONNECTINGTHEWORLD

Why Cybersecurity in Civil Aviation ?

Digitalization is **KEY** to Civil Aviation **INTEROPERABILITY** and Future Development Across **ALL Domains**

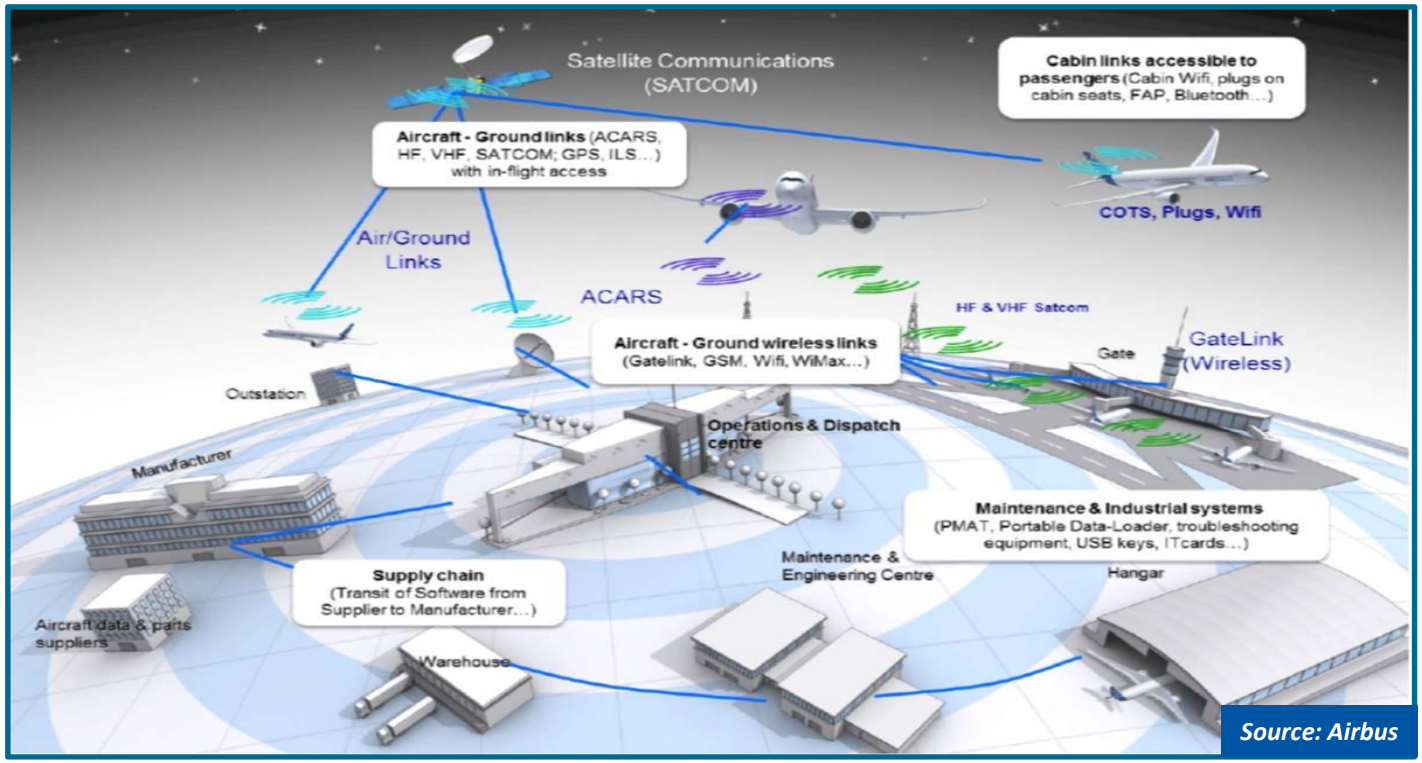
Impact of Technology



ICAO

RECONNECTINGTHEWORLD

Why Cybersecurity in Civil Aviation ?



Source: Airbus

Inter-connection & Interoperability of digital systems between aviation stakeholders **increases cyber threats** by increasing the potential attack surface

ICAO

RECONNECTINGTHEWORLD

Why Cybersecurity in Civil Aviation ?

Why Cybersecurity in Civil Aviation ?

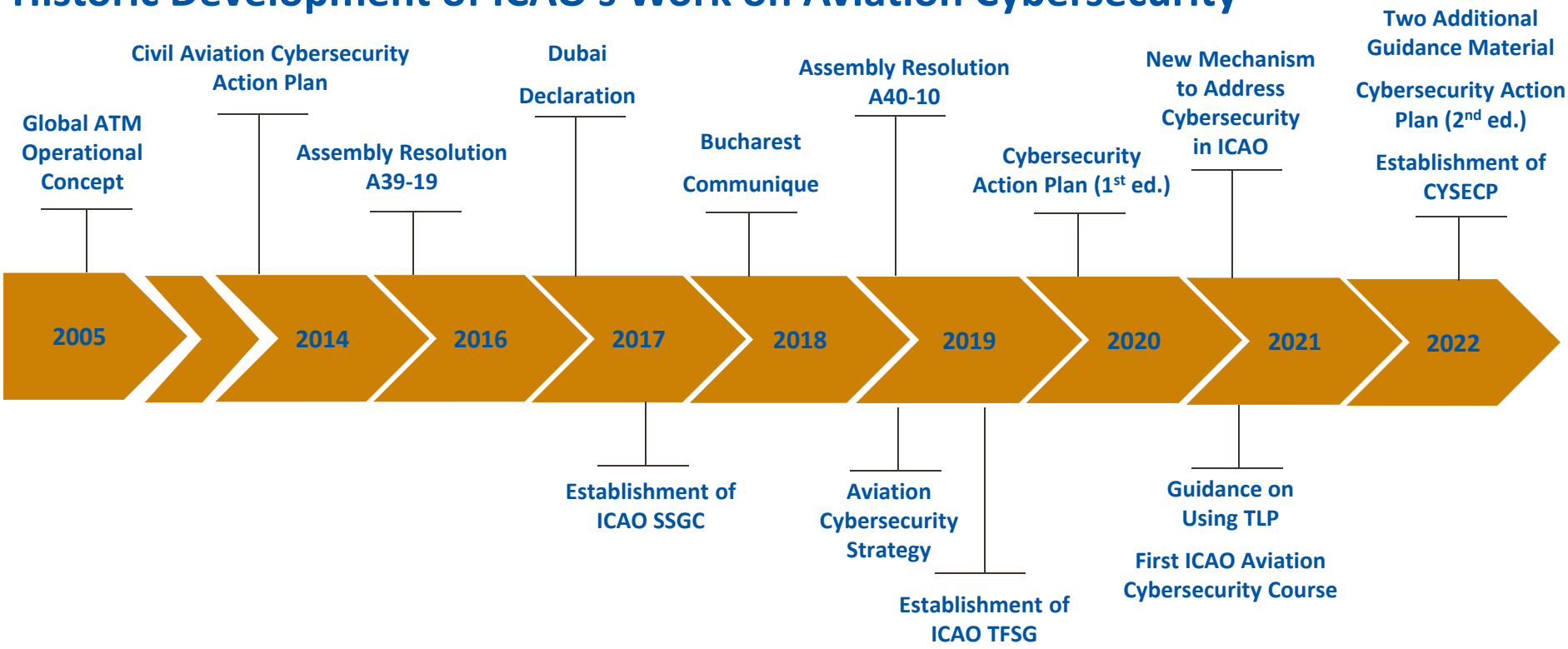
Efforts to address aviation cybersecurity should be:

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

ICAO

RECONNECTINGTHEWORLD

Historic Development of ICAO's Work on Aviation Cybersecurity



ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010

ICAO

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

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

قمع الأفعال غير المشروعة المتعلقة بالطيران المدني الدولي

حررت في بيجين في ١٠ سبتمبر/أيلول ٢٠١٠

BEIJING
10 SEPTEMBER 2010

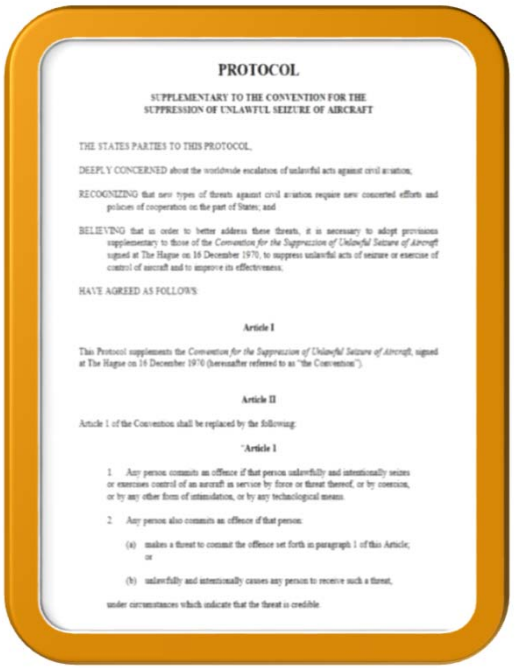
BEIJING
10 SEPTEMBRE 2010

BEIJING
10 DE SEPTIEMBRE DE 2010

ПЕКИН
10 СЕНТЯБРЯ 2010 ГОДА

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

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

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

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

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

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity

ICAO

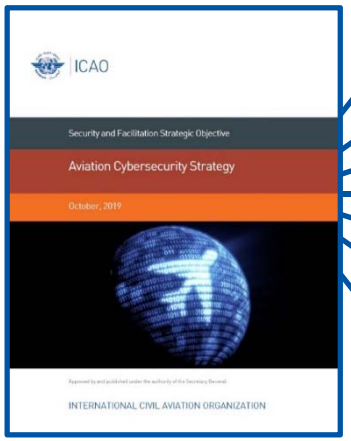
RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

ICAO 40th Assembly Resolution A40 – 10: *Addressing Cybersecurity in Civil Aviation*

- Recognizes that cybersecurity risk can simultaneously affect a wide range of areas;
- Reaffirms the obligations States have under the Chicago Convention;
- Highlights the need for global universal adoption and implementation of the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol);
- Recognizes the need for aviation cybersecurity to be harmonized; and
- Calls upon States to implement the Cybersecurity Strategy.

The 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

The Cybersecurity Action Plan

- **First Edition** published in November 2020.
- **Second Edition** published in January 2022.
- **TLP Green** (asp@icao.int to request a copy) + **Published on ICAO-NET**.
- Provides **the Foundation** for ICAO, States and stakeholders to work together, and proposes a **Series of Principles, Measures, and Actions** to achieve the objectives of the Cybersecurity Strategy's seven pillars.
- **Develops the Seven 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.

The Cybersecurity Action Plan (Examples)

Action #	By	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 2.3	ICAO, Member States, and Industry	Develop guidance material to support organizations in implementing coordinated cybersecurity management frameworks to support the establishment of a systematic approach to manage aviation cybersecurity risks and assess those frameworks' maturity and effectiveness.	Publication of guidelines.	High	2023
CyAP 4.8	ICAO, Member States, and Industry	ICAO to develop risk profiles for each operational domain. Member States and Industry to contribute by developing similar risk profiles at national and organizational levels.	Availability of risk profiles.	High	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
CyAP 6.3	ICAO, Member States, and Industry	Develop guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans.	Publish guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans.	High	2022 - 2023

ICAO

RECONNECTINGTHEWORLD

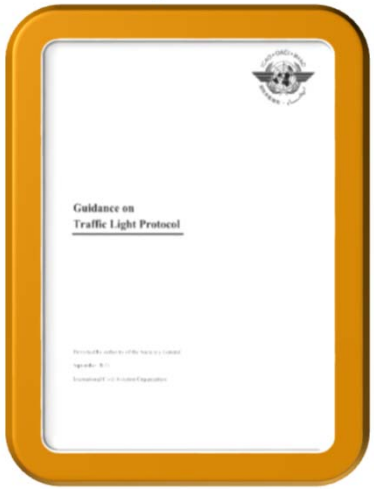
ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Guidance Material:**
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
  - Using Traffic Light Protocol
  - Cybersecurity Culture in Civil Aviation
  - Cybersecurity Policy Guidance

ICAO

RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material



- ✓ Facilitates Cybersecurity information sharing using Traffic Light Protocol.
- ✓ Minimizes Human Error in sharing sensitive information.
- ✓ Supports cybersecurity & Cyber resilience objectives.

- ✓ Calls to focus resources and actions to achieve a systemic approach to cybersecurity in civil aviation.
- ✓ Supports the protection and resilience of international civil aviation's critical infrastructure against cyber threats.

- ✓ Supports the design and implementation of a robust cybersecurity culture in civil aviation.
- ✓ Builds on civil aviation's record in implementing successful aviation safety & aviation security cultures.

ICAO

RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material – Traffic Light Protocol

TLP:RED	**Not for disclosure, restricted to Recipients only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and **could lead to impacts on a party's privacy, reputation, or operations if misused**. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
TLP:AMBER	**Limited disclosure, restricted to Recipients' organizations.** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet **carries risks to privacy, reputation, or operations if shared outside of the organizations involved**. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE	**Disclosure is not limited.** Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

ICAO

RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material – Cybersecurity Culture

- People are the **weakest link** in the cyber chain, **but also** the first line of defense.
- **Cybersecurity Culture is a cornerstone** to protect aviation against cyber threats and hazards.

A Robust aviation cybersecurity culture will complement the sector's efforts in ensuring its Safety, Security, Efficiency, and Resilience.

ICAO

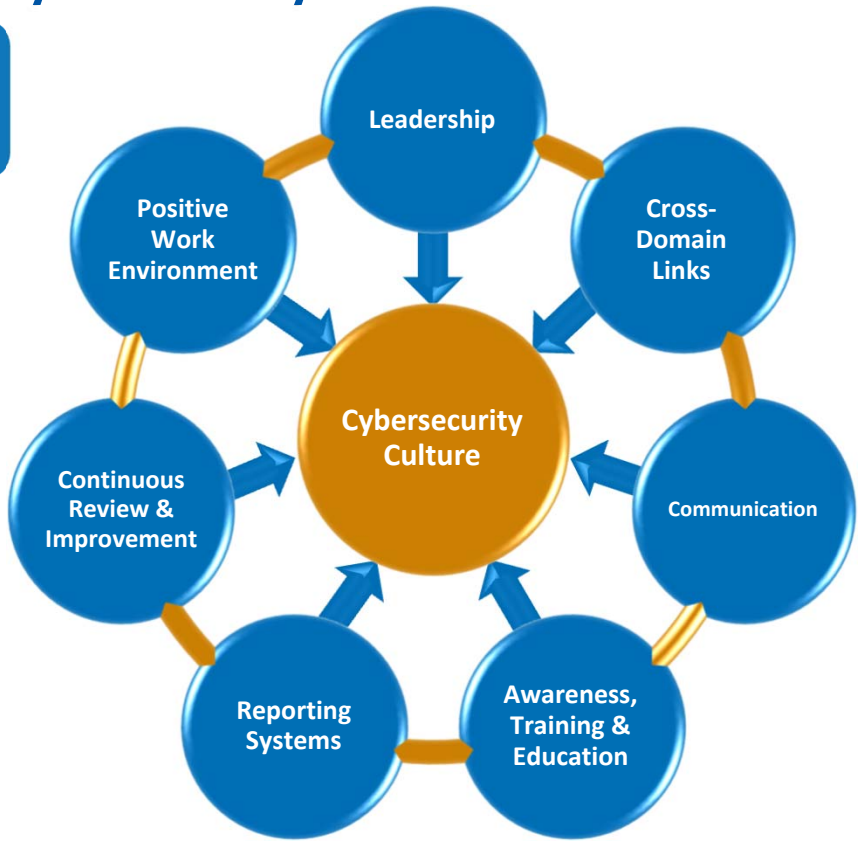
RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material – Cybersecurity Culture

Core Elements of a Robust 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 that supports the effectiveness and efficiency of the organization in mitigating cyber risks.
- enhanced awareness of all personnel to cyber risks and the role that they individually play in identifying and mitigating those risks.
- willingness to report personal oversight in applying organizational cybersecurity processes and procedures as well as reporting of suspicious cyber activities, leading to pro-activeness and better detection of cyber risks.



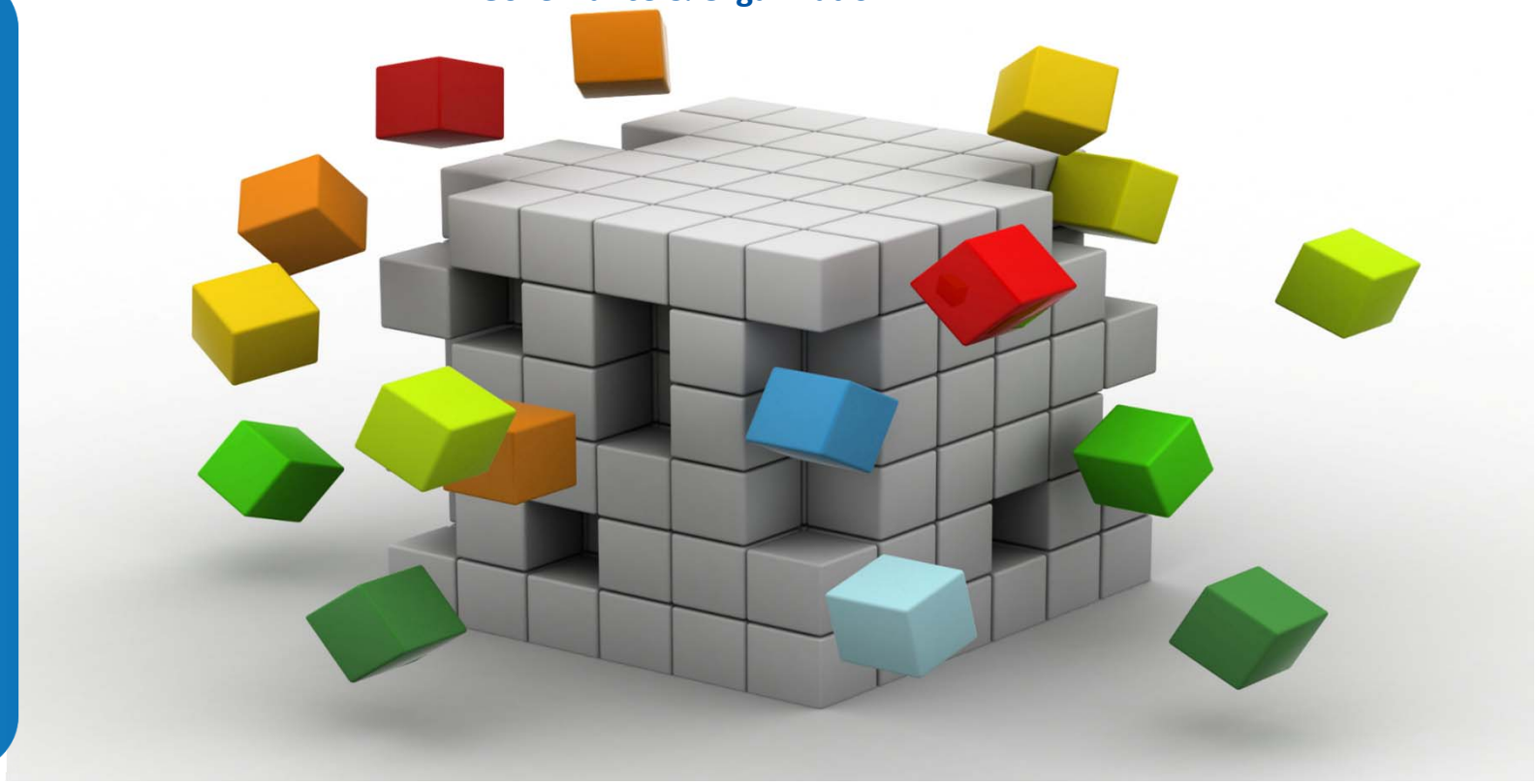
ICAO

RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material – Cybersecurity Policy

Governance & Organization

Main Elements of an Aviation Cybersecurity Policy



Aviation Cybersecurity Guidance Material – Cybersecurity Policy

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

The Appropriate Authority for Aviation Cybersecurity should:

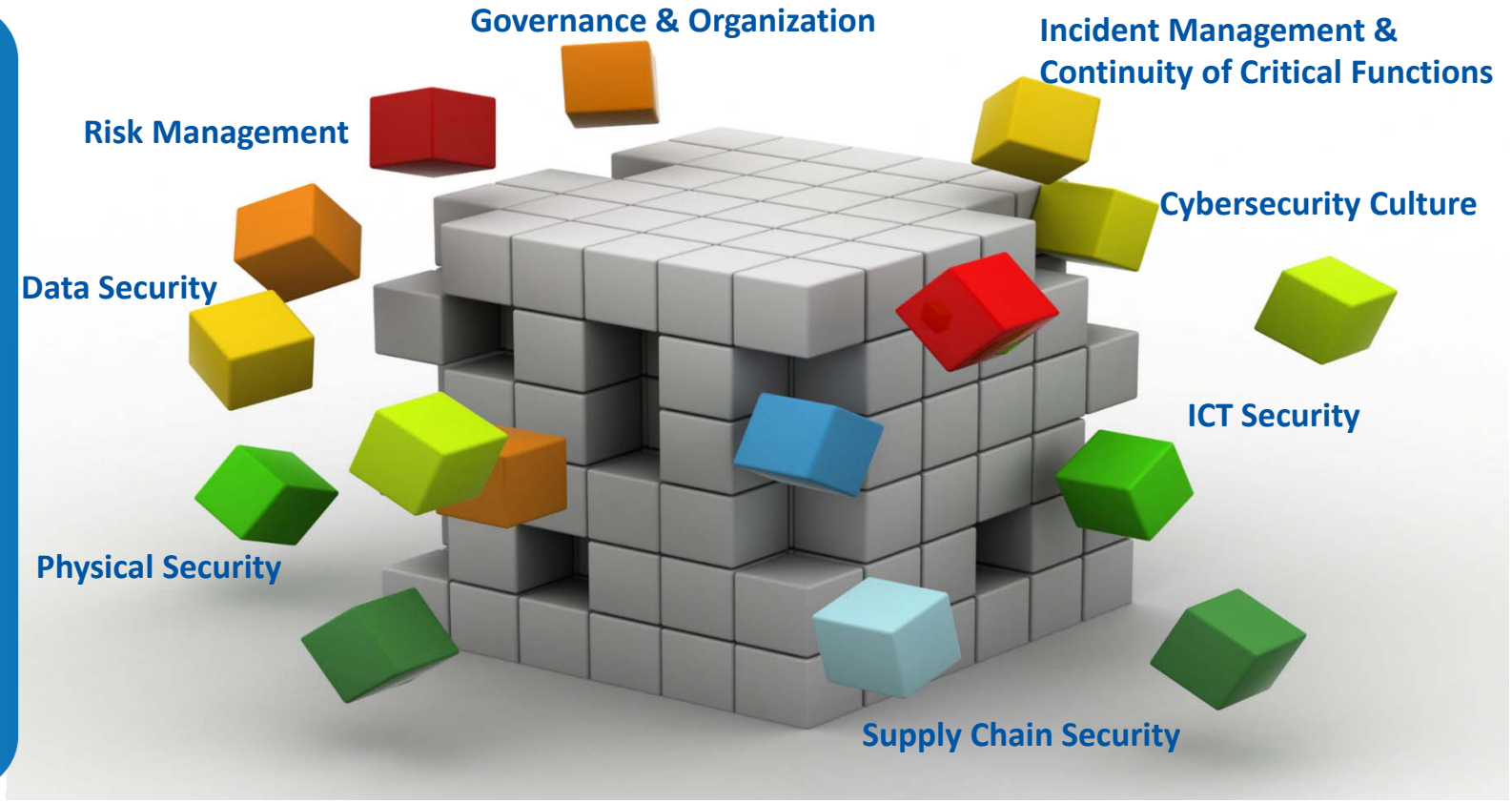
- determine, in coordination with the national competent authority for cybersecurity, the roles and responsibilities to be undertaken by each authority;
- lead the development of aviation cybersecurity regulations;
- clearly define roles and responsibilities for the different civil aviation domains within 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.

ICAO

RECONNECTINGTHEWORLD

Aviation Cybersecurity Guidance Material – Cybersecurity Policy

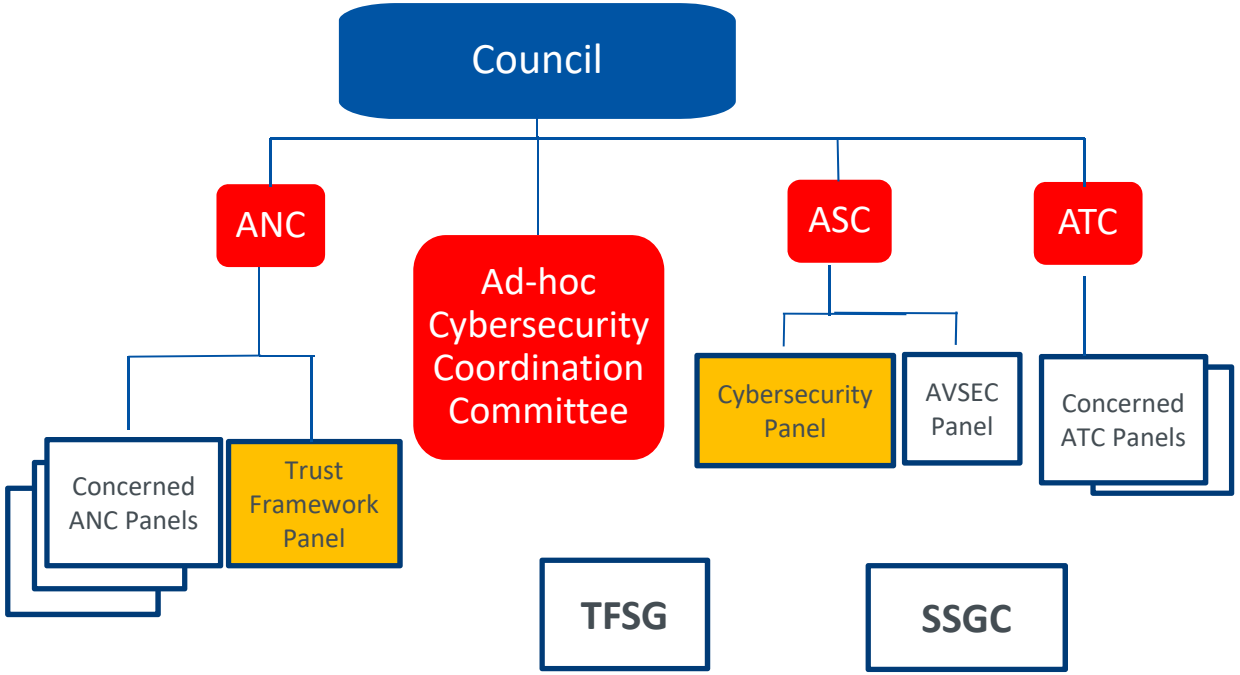
Main Elements of an Aviation Cybersecurity Policy



ICAO

RECONNECTINGTHEWORLD

Enhanced Governance Structure for Aviation Cybersecurity & Cyber Resilience in ICAO



ICAO

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Guidance Material:**
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
  - Using Traffic Light Protocol
  - Cybersecurity Culture in Civil Aviation
  - Cybersecurity Policy Guidance
- **International Aviation Trust Framework (IATF)**

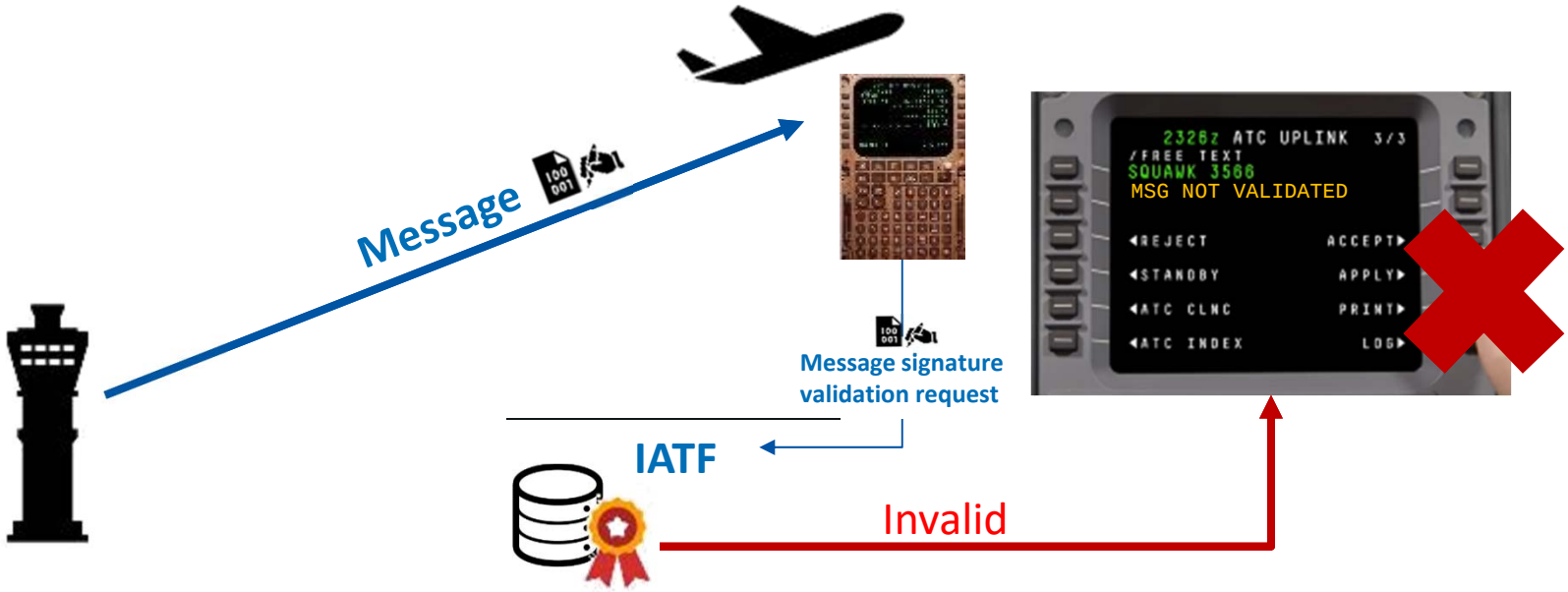
ICAO

RECONNECTINGTHEWORLD

International Aviation Trust Framework (IATF)

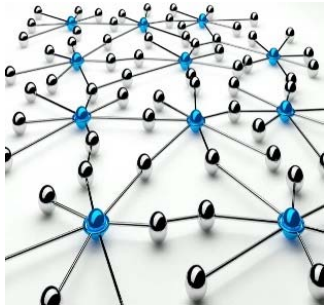
Develop a **common set of principles, policy, and guidance**, and a transition strategy for a **globally harmonized framework** that will **enable trusted** ground-ground, air-ground and air-air exchange of data and information among relevant aviation stakeholders **with the level of resilience and interoperability** needed to support **increased capacity and efficiency for the continued safe operation** of the civil aviation system

International Aviation Trust Framework (IATF)



International Aviation Trust Framework (IATF)

Digital identity



Network

- Technical requirements
- Operational considerations
- Oversight needs

ICAO

RECONNECTINGTHEWORLD

ICAO's Work on Aviation Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Guidance Material:**
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
  - Using Traffic Light Protocol
  - Cybersecurity Culture in Civil Aviation
  - Cybersecurity Policy Guidance
- **International Aviation Trust Framework (IATF)**
- **Training & Capacity Building**

ICAO

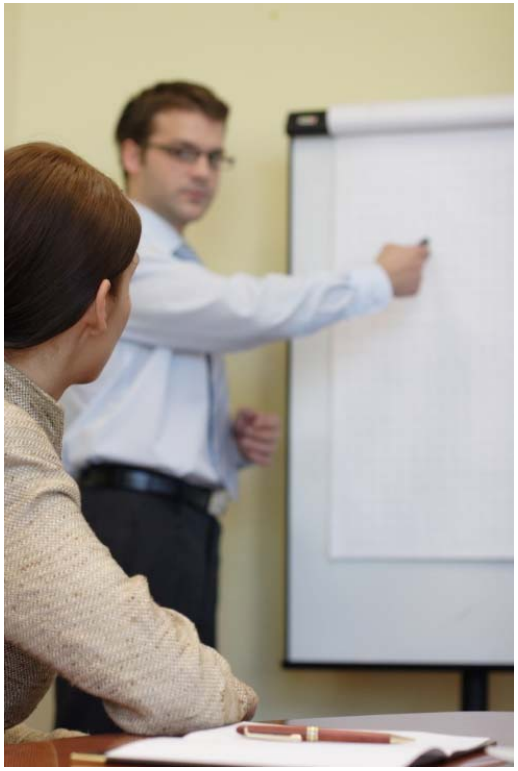
RECONNECTINGTHEWORLD

Training & Capacity Building

- **Foundations of Aviation Cybersecurity Leadership and Technical Management**
  - ✓ Partnership between ICAO and Embry-Riddle Aeronautical University (ERAU)
- **Conducted Sessions**
  - ✓ 4 – 15 October 2021 *(Virtual)*
  - ✓ 6 – 17 December 2021 *(Virtual)*
  - ✓ 14 – 29 March 2022 *(Virtual)*
  - ✓ 23 – 27 May 2022 *(Physical –Frankfurt)*
  - ✓ 27 June – 01 July 2022 *(Physical – Frankfurt)*
- **Planned Sessions**
  - ✓ 3 – 7 October 2022 *(Physical – Singapore)*
  - ✓ 29 October – 4 November 2022 *(Physical – Miami)*

Link to Course *(Upcoming sessions)*

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

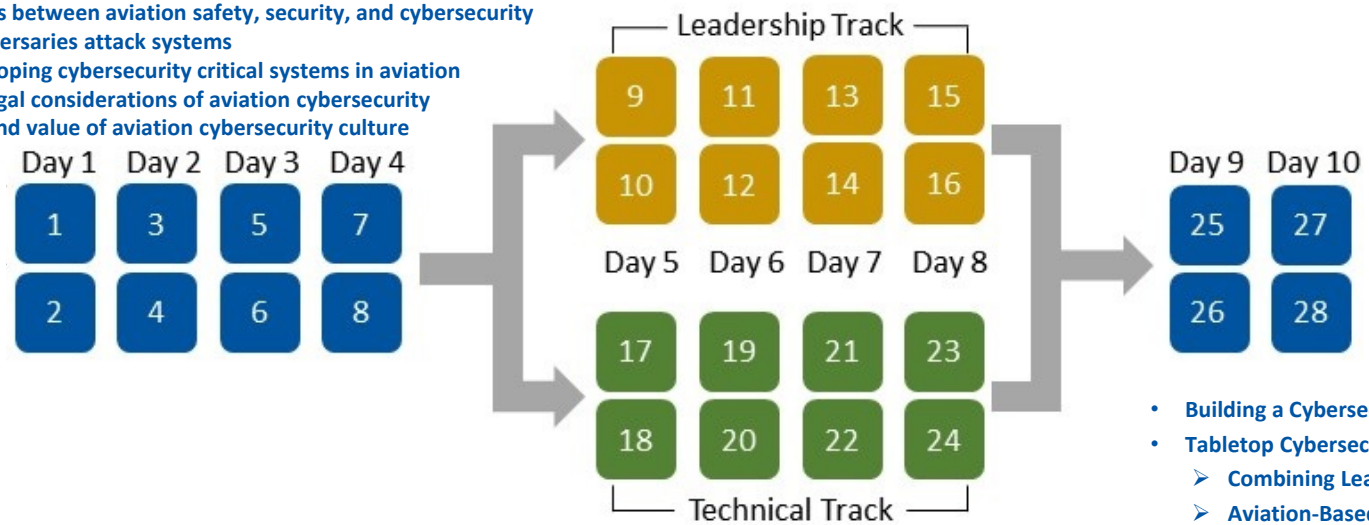


ICAO

RECONNECTINGTHEWORLD

Training & Capacity Building

- How technology underpins all aviation systems
- Interdependencies between aviation safety, security, and cybersecurity
- Why and how adversaries attack systems
- Identifying and scoping cybersecurity critical systems in aviation
- Regulatory and legal considerations of aviation cybersecurity
- The importance and value of aviation cybersecurity culture



- Cybersecurity governance and oversight
- Cybersecurity risk management and assessment
- Managing supply chain risk
- Information sharing
- Staff awareness and training
- Organizational resilience and incident response

- Identity and access management
- Data Security
- System Security
- Resilient networks and systems

- Building a Cybersecurity Strategy
- Tabletop Cybersecurity Incident Exercise
  - Combining Leadership & Technical Aspects
  - Aviation-Based Scenario
  - Brings all Course Elements into Practice

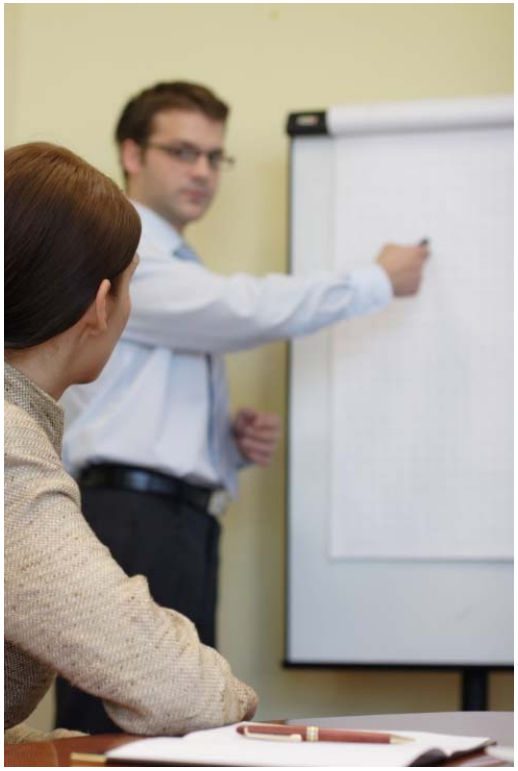
Training & Capacity Building

- **Managing Security Risk in ATM *(Virtual)***
  - Partnership between ICAO and EUROCONTROL.
  - Combines physical security and cybersecurity in ATM.

Finalized & Planned for Delivery (7 to 11 November 2022)

Link to Course Description

https://learningzone.eurocontrol.int/ilp/pages/description.jsf#/users/@self/catalogues/4728296/coursetemplates/11291217/description



- **Cybersecurity Oversight in Aviation**
  - Partnership between ICAO and UK CAAi
  - Focuses on all aspects related to cybersecurity oversight

Under Development for Delivery in 2022 – 2023

ICAO

RECONNECTINGTHEWORLD

The Future?

Digitalization is **ESSENTIAL** for the Growth of the Civil Aviation Sector

Thank You

ICAO