Trust Framework Panel (TFP) Progress Report

Naoki Kanada, Xiaodong Lu

Electronic Navigation Research Institute (ENRI)

National Institute of Maritime, Port and Aviation Technology (MPAT), Japan

The First Meeting of the ANS Information Assurance (ANSIA) Task Force (ANSIA TF/1)

28 – 30 January 2026
Bangkok, Thailand

Overview

- Introduction
- Terms of Reference
- Job Cards
- Working Groups
  - Identity Management
  - Trust Framework Considerations
  - Information Security Framework
- Relationship to the other panels
- Future meeting plans
- Summary

Executive Summary

- Role of Trust Framework Panel
  - Terms of Reference
  - Job Cards
- WG-Identity Management: Doc 10169 Aviation Common Certificate Policy (Accepted to publish)
  - PKI Certificate Policy and Certification Practices Framework
- WG-Trust Framework Considerations: Doc 10xxx Manual on Trust Framework Implementation
  - Use Cases, Beginning Trust Framework Instances
  - WG-TFC: Under Discussion
- WG-Information Security Framework: Doc 10204 Manual on Aviation Information Security (MAIS)
  - Published, but still incomplete
- Future Panel Meeting Schedule

Introduction: Establishment of Trust Framework Panel

- Information and Communication Technology (ICT):
  Critical for Safety and Security of Civil Aviation Operations
- Threats to ICT systems: Safety and Security Risk
- Needs for Addressing Cybersecurity in ICAO Assembly
  - ICAO Assembly Resolution A39-19 (2016)
  - ICAO Assembly Resolution A40-10 (2019)
- Ad-Hoc Cybersecurity Coordination Committee (AHCCC)
  - Established by Council on 15 March 2021 (C-DEC 222nd /11th)
- **Trust Framework Panel (TFP)**
  - Established by Air Navigation Commission (ANC) on 22 June 2022
  - TFP/1: from 27 to 31 March 2023

TFP Terms of Reference (ToR)

- Background
  - Cyber-related events may disrupt the safety and efficiency
- Objectives
  - Develop, address and maintain provisions and guidance materials to support enabling trusted data and information exchange
  - Develop governance principles, policies, procedures and requirements for a globally harmonized framework
  - Define a global architecture and principles for interconnecting networks

TFP Job Cards

- TFP.001.03: Identity Management
  - Identity Management Policies, Procedures and Technical Requirements
- TFP.002.03: Considerations for an International Aviation Trust Framework
  - Consensus among Stakeholders, Governance, and Transition Planning for Trust Framework
- TFP.003.03: Information Security Framework
  - Loss of Confidentiality, Integrity or Availability of the Information poses a Risk for the Safety of Flight Operations
- TFP established Working Group(WG)s for the 3 Job Cards

Working Structure

- ICAO has been examining approaches to enable secure, efficient, and resilient information exchange since 2015.
- Recommendations on cyber resilience (AN-Conf/13 (2018))

Trust Framework Panel

・・・A framework for trusted information exchange

- With the evolution of data and information processing systems, the aviation industry has increasing concerns regarding the effectiveness of existing standards, procedures, and processes for managing risks associated with digital message exchange.
- Cyber-related events may significantly disrupt the safe and efficient provision of aviation services, and reducing cyber-attacks on these systems is a shared objective among all stakeholders.

Three specialized Working Groups (WGs) have been established under the Panel:

WG-Identity Management

Consideration of identity management systems necessary for information exchange

Aviation Common Certificate Policy (ACCP) (Doc 10169)

WG-Trust Framework Consideration

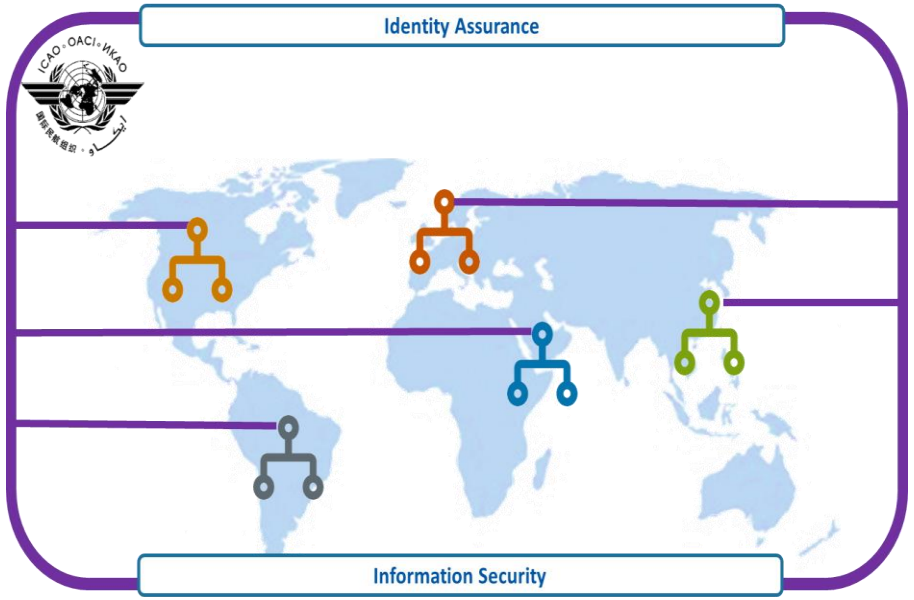
Consideration of technical and operational requirements to establish trust

Trust Framework Manual (Doc XXXXX)

WG-Information Security

Consideration of information security requirements for aviation stakeholders and systems

Manual on Information Security (Doc 10204)



Creating a Chain of Trust

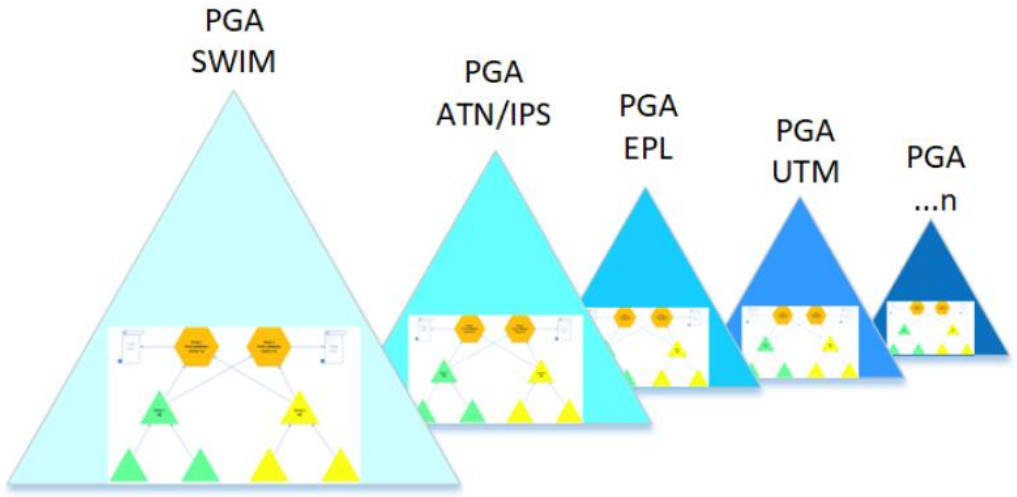
Working Group - Identity Management (WG-IdM)

- ICAO Doc 10169 Aviation Common Certificate Policy (ACCP)
  - Approved by TFP and will be published

ACCP Table of Contents	
Glossary	6. Technical Security Controls
1. Introduction	7. Certificate, CRL and OCSP Profiles
2. Publication and Repository Responsibilities	8. Compliance Audit and Other Assessments
3. Identification and Authentication	9. Other Business and Legal Matters
4. Certificate Life-Cycle Operational Requirements	10. Certificate, CRL and OCSP Formats
5. Facility Management and Operations Controls	11. Smartcard Profiles (TBD)

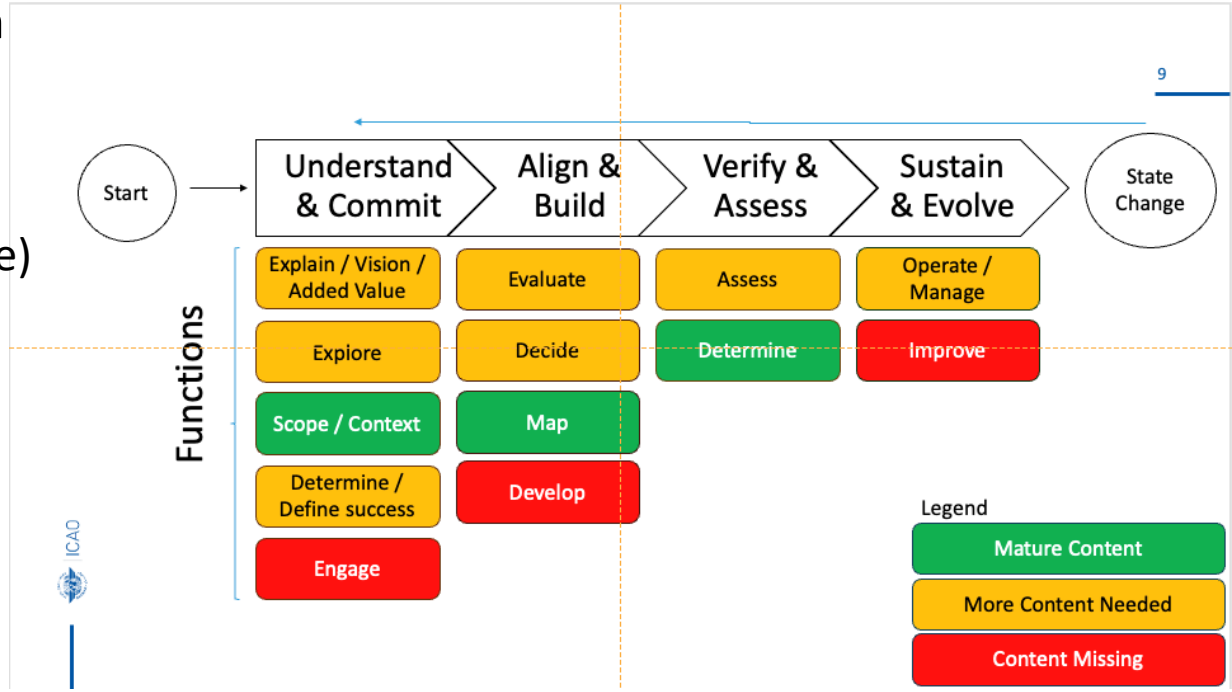
Doc 10169 Aviation Common Certificate Policy

- X.509 Public Key Infrastructure (PKI) Certificate Policy (CP) and Certificate Practices Statement (CPS)
  - Civil Aviation version of RFC3647:
    X.509 PKI Certificate Policy and Certification Practices Framework
  - CP: PKI Policy and Requirements
  - CPS: Procedure for Certificate Authority
- From the International Aviation Trust Framework (IATF) to Trust Framework Instances (TFIs)
  - IATF: Centralized and International
  - TFIs: Federated and Self-Governed
- Harmonization and Interoperability



Working Group - Trust Framework Considerations

- Use Cases for Trust Framework Instances Classification
  - Information exchange (e.g. SWIM)
  - Communication (e.g. CPDLC)
  - Person or equipment authentication (e.g. Digital License)
  - Navigation System (e.g. SBAS)
- How to make a TFI: TFI lifecycle
  - Under Discussion
  - Detailed in different paper
- Behind Schedule due to transition from IATF to TFIs



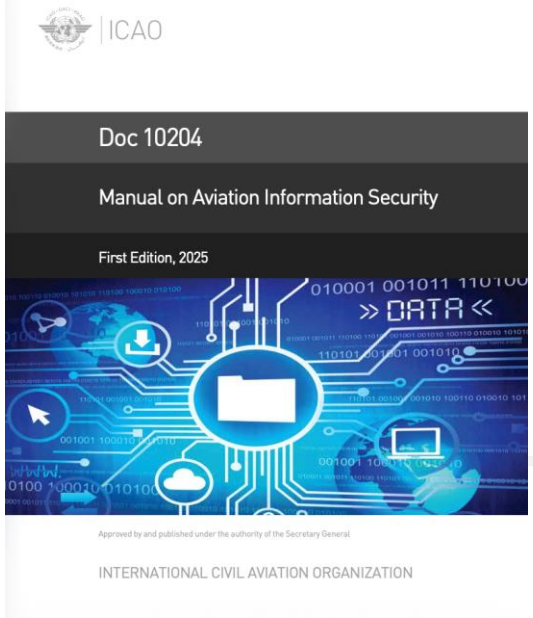
Working Group - Information Security Framework

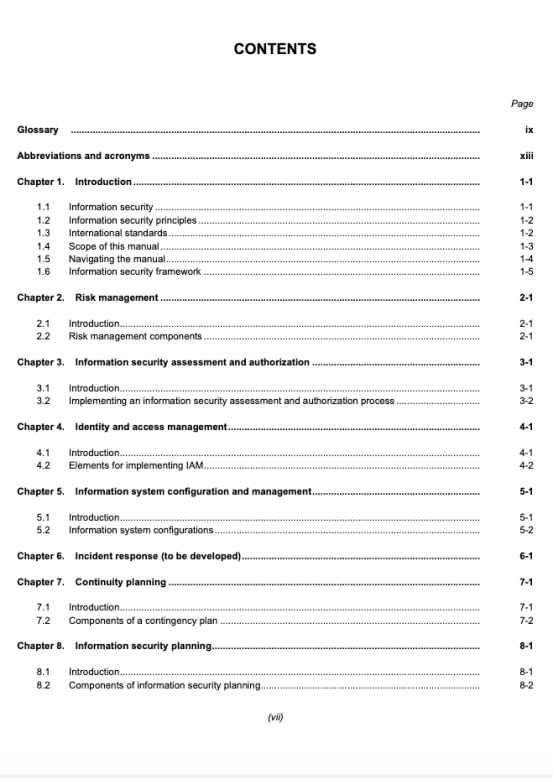
- ICAO Doc 10204 Manual on Aviation Information Security (MAIS): published

MAIS Table of Contents	
Glossary	9. Configuration Management
1. Introduction	10. Continuous Monitoring (TBD)
2. Risk Management	11. Information System Maintenance
3. Information Security Assessment and Authorization	12. Security in Software Development (TBD)
4. Identity and Access Management	13. Supply Chain Risk Management
5. Information System Configuration and Management	14. Media Protection
6. Incident Response (TBD)	15. Physical and Environmental
7. Continuity Planning	16. Personnel Security
8. Information Security Planning	17. Information Security Awareness and Training (TBD)

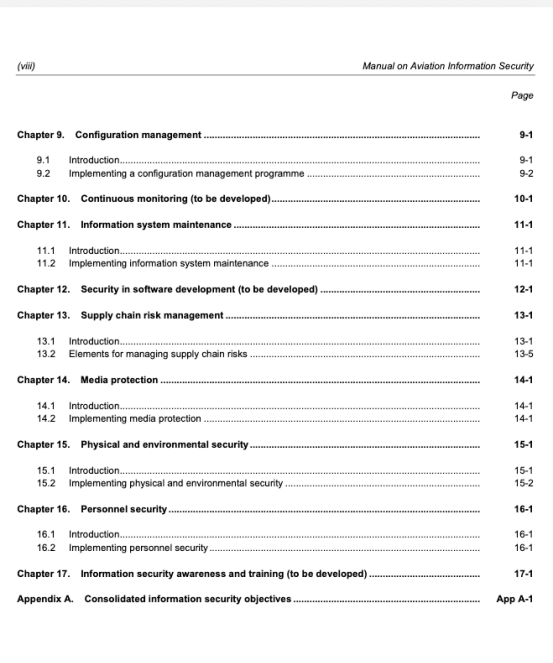
Manual on Aviation Information Security (MAIS)

- Information Security Management System (ISMS) for Civil Aviation
- Some Chapters are not complete
  - 6. Incident Response (from CYSECP)
  - 10. Continuous Monitoring
  - 12. Security in Software Development
  - 17. Information Security Awareness and Training
- Difference between MAIS and ISMS
  1. Purpose of MAIS is Aeronautical Safety
     = an Information Security Risk is the Safety Risk
  2. ISMS: Part of Internal Control
     MAIS: Information Exchange among Multiple Organizations
- Current Status
  - Incident Response and Training Chapter from CYSECP
  - Developing Software Development Chapter



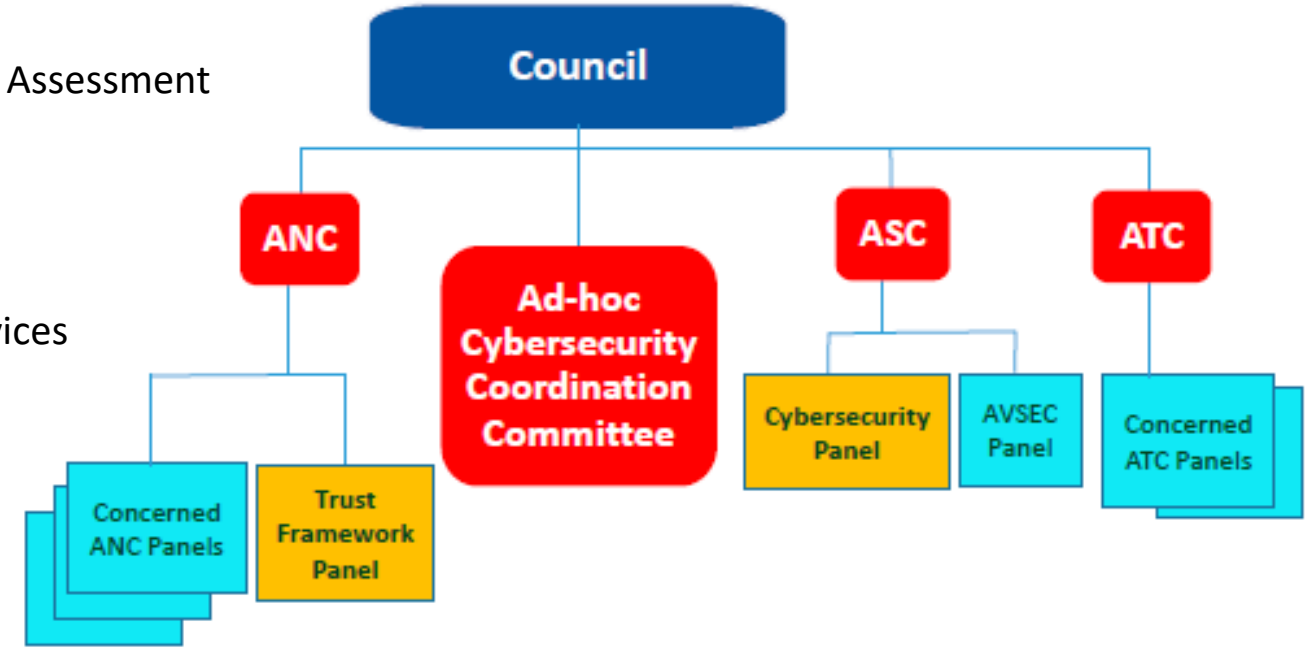

CONTENTS

(vii)



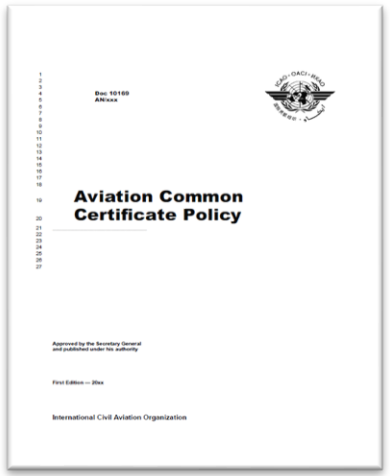
TFP Relationship to Other Panels

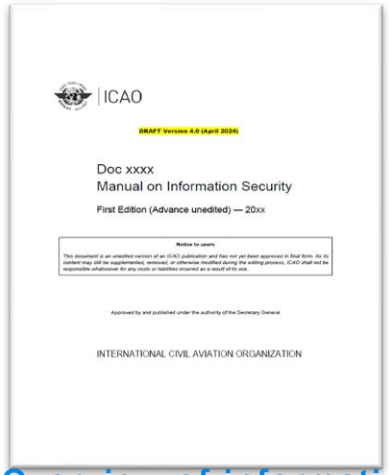
- Ad-Hoc Cybersecurity Coordination Committee (AHCCC): Coordination under Council
- Cybersecurity Panel (CYSECP): Cyber version of Aviation Security Panel (AVSEC), based on ICAO Annex 17
- Communications Panel Data Communication Infrastructure Working Group (CP-DCIWG)
  - WG-I (Internet) Internet Protocol Suite (IPS) Security SG
    - Security Risk Assessment
      Doc 10145: Manual on Aeronautical Security Risk Assessment
    - IPS PKI Certificate Policy
      Doc 10095: Manual on PKI Policy for ATN/IPS
    - ATN/IPS Security Framework
      Doc 10090: Manual on Aeronautical Security Services
- Information Management Panel (IMP)
  - WG-G (Governance)
- Navigation Systems Panel (NSP)
  - SBAS Authentication Ad-hoc Group (SAAG)



Relationship with PANS-IM

Chapter	Overview
PANS-IM, Chapter 6	All information management stakeholders responsible for generating, storing, consuming, or transferring information shall implement an Information Security Framework designed to ensure the confidentiality (when required), integrity, and availability of information and information services.
	The Information Security Framework shall be applied in an integrated manner across networks, technical infrastructure, information, information services, and applications.
	Information service providers shall classify information in accordance with defined information security categories in order to achieve a mutual understanding of the protection level of exchanged information.





Future meeting plan

- TFP/3: From 2026-03-30 to 2026-04-02 (Montreal)
- TFP-WG/4: From 2026-09-14 to 2026-09-18 (TBD:Brazil?)
- TFP/4: From 2027-05-03 to 2027-05-07 (Montreal)
- TFP-WG/5: From 2027-09-13 to 2027-09-17 (TBD)
- TFP/5: From 2028-05-22 to 2028-05-26 (Montreal)
- TFP/6: From 2029-05-14 to 2029-05-18 (Montreal)

Trust Framework Panel Summary

- Objectives
  - Develop, address and maintain provisions and guidance materials to support enabling trusted data and information exchange
  - Develop governance principles, policies, procedures and requirements for a globally harmonized trust framework
- Doc 10169 Aviation Common Certificate Policy
  - PKI Policy, Requirements
  - Procedures for Certificate Authorities
- Doc 10xxx Manual on Trust Framework Implementation
  - Explanation and Use Cases of Trust Framework Instances
- Doc 10204 Manual on Aviation Information Security
  - Information Security Management for Safety Management