



ICAO

International Civil Aviation Organization

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

Bangkok, Thailand, 28 – 30 January 2026

Agenda Item 4: Global and Regional Trust Framework updates

PRE-REQUISITES TO TRUST FRAMEWORK INSTANCE PARTICIPATION

(Presented by Singapore)

SUMMARY

This information paper presents an update to the ANS Information Assurance Task Force on the pre-requisites to the participation of any Trust Framework Instance and how ANSIA Task Force Members can prepare for the eventuality of a Trust Framework Instance within the APAC region.

1. INTRODUCTION

1.1 At the 10th meeting of the ICAO APAC System-Wide Information Management (SWIM) Task Force, Japan presented a paper, WP/15 Requirements for Implementing Aviation Information Security Framework at the APAC Region

1.2 The paper described the requirements in implementing an aviation security framework. It references the work done by the ICAO Trust Framework Panel (TFP), ICAO Doc 10169: Aviation Common Certificate Policy (ACCP), and ICAO Doc 10204: Manual for Aviation Information Security (MAIS).

1.3 The paper also proposed the following:

- Considerations for PKI implementation within the APAC region;
- A working group or task force to looking into the development of a regional federated Public Key Infrastructure architecture; and
- A technical community to support the implementation of Trust Framework Instances (TFI), in which SWIM is just one of many potential use cases.

2. DISCUSSION

2.1 The TFP is in the midst of drafting a third document, known as the Trust Framework Manual (TFM). The purpose of the TFM, as drafted today, is to provide a guide in establishing, implementing and managing a TFI within the global aviation sector.

2.2 The TFM also serves to tie the two other materials produced by the TFP, ICAO Doc 10169 ACCP and ICAO Doc 10204 MAIS. The two documents serve as the pre-requisites to the usage of the TFM, and hence pre-requisites to the formation or participation of any TFI.

2.3 The ACCP helps establish assurance levels for the aviation sector, promoting interoperability across Certificate Authorities (CAs) and other PKI domains

2.4 The MAIS provides guidance to information system owners to implement information security objectives as defined in the MAIS.

2.5 As part of the requirements of any participation in any TFI, 2 major pieces of information from every organisation that wants to be part of any TFI are required:

- An organisation's Certificate Policy (CP). This is a set of rules that defines the issuance and management of digital certificates within a PKI, governing the trust relationships between entities.
- An organisation's Information Security Management System (ISMS). This is a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability through security controls and procedures.

2.6 The organisation's CP will be used to map against the ACCP. This is done to establish a baseline to check against for compliance in any TFI.

2.7 The organisation's ISMS will be used to map against the MAIS. This mapping is done to establish a baseline which provides insights as to whether an organisation's current security measures are sufficient for the organisation to be part of any TFI.

2.8 The current proposed standards in the TFM draft, which are still subjected to changes, for an organisation's CP are as follows:

- RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile
- ISO/IEC 9594-8 / ITU-T X.509 – Standard for defining certificates and public key infrastructure.
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- NIST SP 800-57 - Recommendation for Key Management
- ETSI EN 319 411-1/2 - Electronic Signatures and Infrastructures

2.9 The current proposed standards in the TFM draft, which are still subjected to changes, for an organisation's ISMS are as follows:

- ISO/IEC 27001 - Information Security Management Systems (ISMS) - Requirements
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- ISO/IEC 27005 - Information security risk management
- ISO/IEC 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 - Protection of personal data in the cloud
- NIST SP-800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-11 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- CIS Controls
- GDPR – General Data Protection Regulation

- SOC 2 – Service Organization Control 2

2.10 When an organisation completes the two mappings, they serve as the basis to determine if an organisation is able to be participate in any TFI.

2.11 Any future technology enhancements to security due to future technology, such as Quantum Cryptography, will necessarily be included as enhancements to the ACCP, MAIS and the Trust Framework Manual in future editions.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

- a) note the information contained in this paper;
- b) consider the status of their own organisation’s Certificate Policy, and Information Security Management System;
- c) discuss any relevant matter as appropriate
