ICAO UNITING AVIATION

Information security requirements for exchange of information over IP

APAC CNS SG/25
October 2021

Ms. Olga De Frutos Martin
TO AN, ANB, ICAO

Flight Plan

- PANS-IM
- Information Security Framework

ICAO PROVISIONS

- Draft PANS-IM (Doc XXXX)
  - SWIM
  - Quality
  - Governance
    - Need
    - Implementation Framework
  - Information
    - Information exchange models
    - Metadata
  - Information services
    - Information Service Overview
    - Information Service Publication
    - SWIM Service Registry
  - Technical Infrastructure
    - IP Network
    - Interface bindings
    - Information Security Framework

- Information services on
  - Meteorological information
    - Future amendment to Annex 3
  - Aeronautical Information
    - Future amendment to Annex 15 and PANS-AIM
  - Flight and Flow Information
    - Future amendment to PANS-ATM

- Guidance material
  - To support the implementation of the SARPs and PANS

INFORMATION SECURITY FRAMEWORK

- Layered approach
- **Minimum** requirements to ensure **trust**
  - Information integrity, availability and confidentiality
- Scalable
  - Based on the criticality of the information to be exchanged and the size of the organization
- Common practices based on NIST and ISO
  - NIST and ISO are not measurable
  - Harmonization (as required in the SWIM concept) and tailored to aviation
- Performance based, implementation agnostic and SMART requirements

INFORMATION SECURITY FRAMEWORK

- Scope
  - Broader than SWIM
    - Organizations **exchanging** information, that may have an impact on safety, over an IPS-based network
    - Organizations may refer to information service providers or information service consumers if the exchange of information is bi-directional
  - End-to-end information security
    - To provide for end-to-end information security, performance-based information security requirements shall be applied to the technical infrastructure, the network on which the technical infrastructure is based, the information, the information service and the applications in an integrated manner.

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - IPv6 dedicated block of addresses
    - Reduce attack surface

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - IPv6 dedicated block of addresses
    - Organizations shall use addresses from the aviation dedicated block of IPv6 addresses.
    - Organizations who wish to manage their own IPv6 address sub-block from the aviation dedicated block of IPv6 addresses, shall develop a plan for making sub-allocations to other IPv6 address users within their organization to qualify for an initial allocation of an aviation IPv6 address sub-block. The plan shall project the IPv6 address usage for a minimum of two years.

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - Fully qualified DNS service
    - Mitigation of spoofing and denial of service attacks

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - Fully qualified DNS service
    - Organizations shall use a name from a fully qualified Domain Name System (DNS).

INFORMATION SECURITY FRAMEWORK

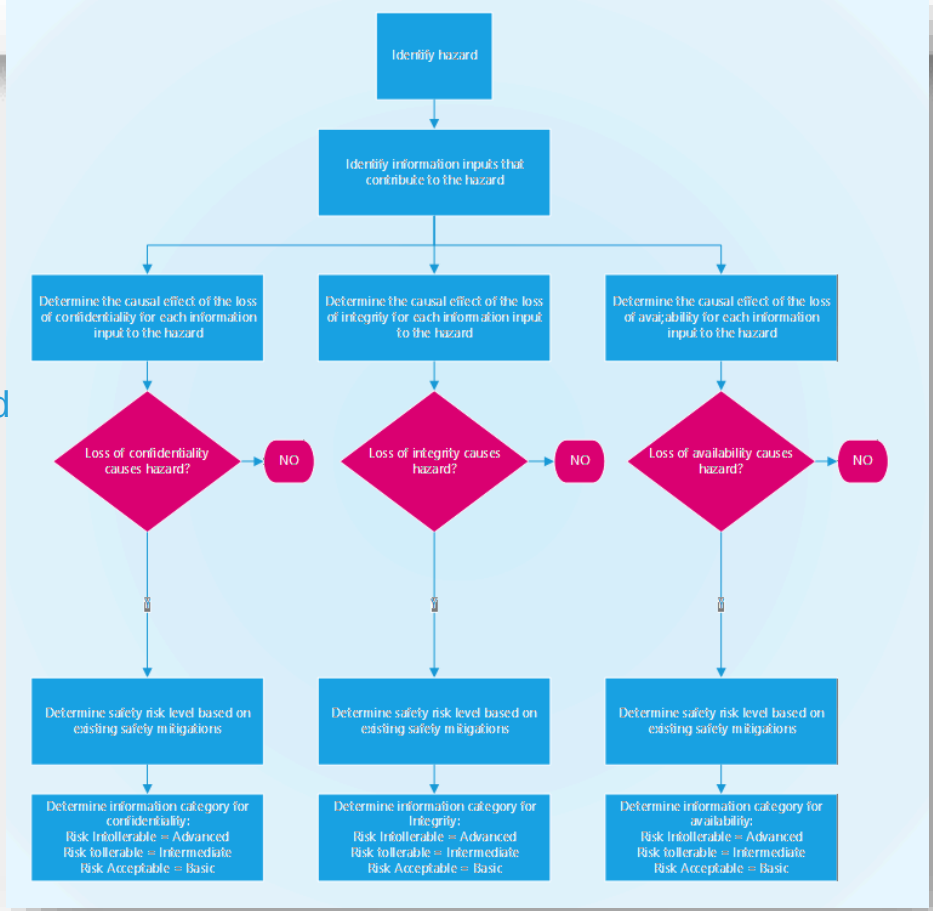
- Layered approach
  - Impact of the loss of information security on safety
    - To have a mutual understanding of the level of information protection provided
    - Different type of information require different type of protection based on the **acceptable level of safety risk taken** for the use **of the information**
    - Information security categories
      - *None, basic, intermediate and advanced*
      - Methodology for the categorization of information → Safety Management Manual
      - Application of a minimum set of performance-based standards based on the category of the information → Appendix to PANS-IM

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - Impact of the loss of information security on safety
    - Organizations shall classify the information according to defined information security categories to ensure a mutual understanding of the level of protection of the information exchanged. Information security categories may differ between information service providers and consumers.

      Note. – See Safety Management Manual (Doc 9859) for classification of information in the defined information security categories.

- Safety Management Manual
  - Information security hazards can modify the likelihood of the safety risk based on the capability of the malicious actor and the likelihood of the attack based on threat intelligence.
  - Safety risk mitigation of information security hazards requires:
    - The identification of information security hazards
    - The identification of information inputs that contribute to the hazard
    - The determination of the causal effect of loss of confidentiality, integrity or availability on the information inputs identified.



INFORMATION SECURITY FRAMEWORK

- Layered approach
  - Impact of the loss of information security on safety
    - Information service providers shall state the information security category in the Information security category metadata field of the information service overview to provide information service consumers with an understanding of the level of protection of the information.
    - Organizations should consider the implementation of the requirements in Appendix A based on the information security category stated in the Information security category metadata field of the information service.

Note. – For more information on the implementation of the requirements in Appendix A see Information Security Manual.

- Appendix A to PANS-IM

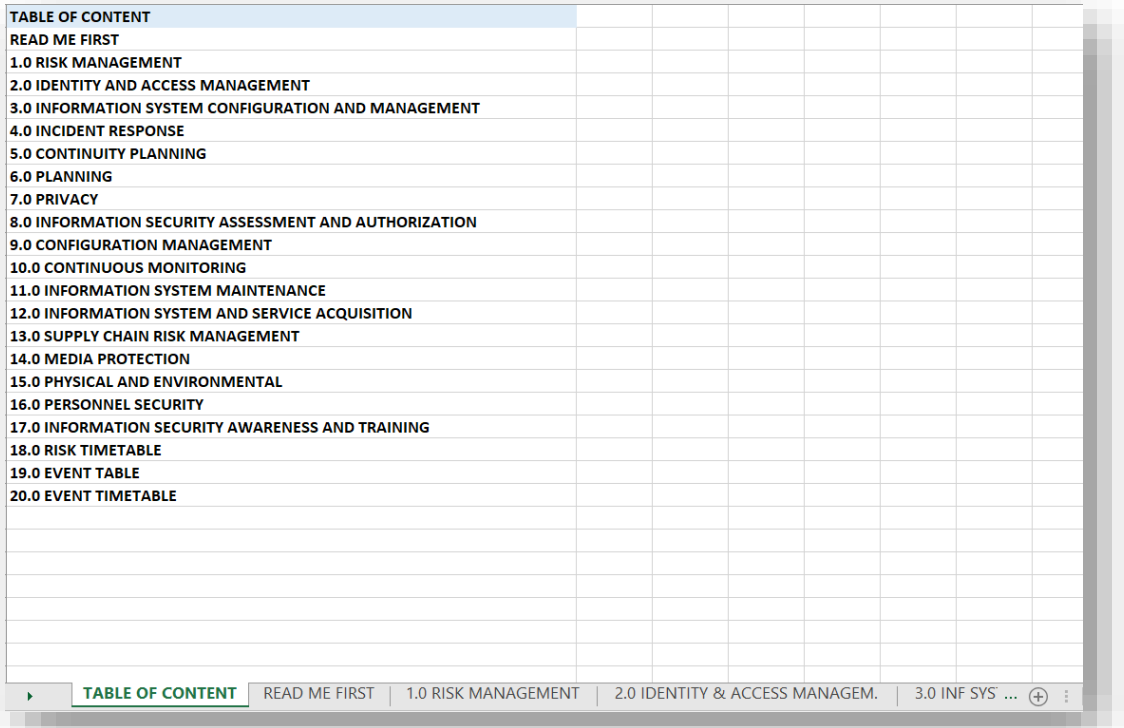


TABLE OF CONTENT
READ ME FIRST
1.0 RISK MANAGEMENT
2.0 IDENTITY AND ACCESS MANAGEMENT
3.0 INFORMATION SYSTEM CONFIGURATION AND MANAGEMENT
4.0 INCIDENT RESPONSE
5.0 CONTINUITY PLANNING
6.0 PLANNING
7.0 PRIVACY
8.0 INFORMATION SECURITY ASSESSMENT AND AUTHORIZATION
9.0 CONFIGURATION MANAGEMENT
10.0 CONTINUOUS MONITORING
11.0 INFORMATION SYSTEM MAINTENANCE
12.0 INFORMATION SYSTEM AND SERVICE ACQUISITION
13.0 SUPPLY CHAIN RISK MANAGEMENT
14.0 MEDIA PROTECTION
15.0 PHYSICAL AND ENVIRONMENTAL
16.0 PERSONNEL SECURITY
17.0 INFORMATION SECURITY AWARENESS AND TRAINING
18.0 RISK TIMETABLE
19.0 EVENT TABLE
20.0 EVENT TIMETABLE

Note - The requirements in this section are not applicable when delay due to authentication or session termination can cause a safety risk on the operations. These exceptions shall be documented in the Identity and Access management policy and shall include alternative or compensating information security controls

ID	OBJECTIVE	DESCRIPTION	BASIC	INTERMEDIATE	ADVANCED	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
2.1	Identity and Access Management Policy and Procedures	Organizations shall develop, disseminate within the organization, and periodically update an identity and access management policy and related procedures.	Identity and access management shall be part of a general information security policy and procedures.	Identity and access management shall have a dedicated policy with related procedures which shall be reviewed every two (2) years or when circumstances require such a review (e.g. regulatory change, a new operational context, incident, etc.).	Identity and access management shall have a dedicated policy with related procedures which shall be reviewed annually or when circumstances require such a review (e.g. regulatory change, a new operational context, incident, etc.).	X	X	
2.2	Identity Management	Organizations shall identify employees, individuals acting on behalf of the organization (e.g. contractors, guest researchers, etc.), systems and all users who require access to information systems under their responsibility for privileged and non-privileged functions.	Identities for employees, individuals acting on behalf of the organization, systems, and all users shall be established at minimum at an identity assurance Level 2 (See chapter 1 Definitions).	Identities for employees, individuals acting on behalf of the organization, systems, and all users shall be established at minimum at an identity assurance Level 3 (See chapter 1 Definitions).	Identities for employees, individuals acting on behalf of the organization, systems, and all users shall be established at minimum at an identity assurance Level 4 (See chapter 1 Definitions).	X	X	
2.3	Separation of Duties	Organizations shall establish and document separation of duties for privileged functions.	Access to privileged functions shall be controlled with privileges that minimize the risk of collusion.	Privileged functions shall be assigned based on information system functions (e.g. network, database, etc.) to different employees or individuals acting on behalf of the organization.	Privileged functions shall be assigned based on information security functions (e.g. network, database, etc.). The assignment shall ensure that employees or individuals acting on behalf of the organization only have a single role per access management system.	X	X	
2.4	Account Management	Organizations shall identify and assign information system administrators. Information system administrators are responsible for: assigning and designating privileges to groups and roles for privileged and non-privileged accounts; and approving, monitoring. They are also responsible for periodically reviewing privileged and non-privileged accounts.	Information systems shall have designated administrators to: assign privileges to groups and roles for privileged and non-privileged accounts; review and approve requests for privileged and non-privileged accounts; and perform account reviews periodically. Information systems shall produce audit trails with account actions and time stamps.	Information systems shall have designated administrators to: assign privileges to groups and roles for privileged and non-privileged accounts; review and approve requests for privileged and non-privileged accounts; and perform quarterly account reviews. Information systems shall produce audit trails with account actions and time stamps.	Information systems shall have designated administrators to: assign privileges to groups and roles for privileged and non-privileged accounts; review and approve requests for privileged and non-privileged accounts; and perform monthly account reviews. Information systems shall produce audit trails with account actions and time stamps.	X	X	

INFORMATION SECURITY FRAMEWORK

- Layered approach
  - Impact of the loss of information security on safety
    - Safety refers to the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level. The loss of confidentiality, integrity and availability of the information may impact safety. Therefore, information service consumers shall assess the impact of the loss of confidentiality, integrity and availability of the information on safety to determine the information security category required for the operational use of the information.

Note – See Safety Management Manual (Doc 9859) for the assessment of the impact of the loss of confidentiality, integrity and availability of the information on safety and classification of information in information security categories.

ICAO


North American Central American and Caribbean (NACC) Office
Mexico City
South American (SAM) Office
Lima
ICAO Headquarters
Montréal
Western and Central African (WACAF) Office
Dakar
European and North Atlantic (EUR/NAT) Office
Paris
Middle East (MID) Office
Cairo
Eastern and Southern African (ESAF) Office
Nairobi
Asia and Pacific (APAC) Sub-office
Beijing
Asia and Pacific (APAC) Office
Bangkok
THANK YOU