APIRG
INFRASTRUCTURE & INFORMATION (IIM) SUB-GROUP
COMMUNICATION PROJECT 5

Africa-Indian Ocean (AFI) Region Air Navigation Services Cyber Resilience Framework

Document information	
APIRG Subgroup	Infrastructure & Information Management APIRG Sub Group
Project Title	Assessment of AFI Air Navigation Services Cyber Resilience
Project Number	IIM SG Communication Project n°5 (COM 5)
Project Coordinator	Côte d'Ivoire
Deliverable Name	AFI Air Navigation Services Region Resilience Framework
Deliverable ID	D07
Edition	00.02.02
Tasks Contributors	
ASECNA, Benin, Cameroon, Côte d'Ivoire, Gambia, Ghana, IATA, Kenya, Nigeria, South Africa, Somalia, Madagascar	

Document History

Edition	Date	Status	Author	Justification
00.00.01	04/11/2018	Initial Draft	F. JUMA	New Document Initial scope of the AFI ANS Cyber resilience Framework
00.00.02	10/07/2019	Draft	F. JUMA N. LEKOTA (ATNS) S. GNASSOU (ANAC CI) A. CUMBI (ASECNA)	Update of all the document following the first review by the project team
00.00.03	29/07/2019	Draft	F. JUMA N. LEKOTA S. GNASSOU	Update of all sections following the second internal review by all the project team
00.00.04	27/09/2019	Draft	All the project team	Update of chapter 1, 2,3,
00.00.05	23/12/2019	Final Draft	F. JUMA N. LEKOTA S. GNASSOU	Update of all sections to consider the recommendations from the AFI Cyber safety and resilience workshop with tabletop exercise (AFI TTX) (AFI CSRW), 3rd to 5th December 2019, Nairobi
00.01.00	27/01/2020	Consolidated Edition	All IIM SG COM Project 5 team	Finalization of the framework by the project team following the last review period Consolidated edition submitted to IIM Chairperson and Secretariat for final review and approval (31/01/2020)
00.01.00	30/03/2021	Revised edition	S. GNASSOU	Update of chapter 1
00.01.01	30/07/2021	Revised edition	F. JUMA S. GNASSOU	Update of list of references (new guidelines)
00.01.02	30/12/2021	Revised edition	S. GNASSOU	
00.01.03	01/03/2022	Revised edition	All IIM SG COM Project 5 team	Alignment with the developments in the cyber threats landscape as well as the technological developments within the civil aviation sector (Cybersecurity Action plan second edition January 2022, Cybersecurity Policy guidance) Update of chapters 2, 3 and 5
00.01.04	24/05/2022	Revised edition	IIM SG COM Project 5 team	Integration of corrections made by the IIM COM 5 team following the final internal review (April/ May 2022)
00.01.05	03/06/2022	Revised edition	IIM SG COM Project 5 team	Update of list of cyber threats to civil aviation
00.02.00	13/11/2022	Revised edition	PTC	Finalization of 2022 Update for submission to IIM chair and Secretariat
00.02.01	31/12/2022	Final 2022 edition	IIM COM5 PTC	Finalization of 2022 Update for submission to IIM chair and Secretariat
00.02.01	31/03/203	Final 2023 edition	F. JUMA S. GNASSOU	2023 Update for submission to IIM chair and Secretariat

Foreword

This document was developed with the assistance of the APIRG IIM Subgroup with the aim of assessing AFI Air Navigation Services Cyber Resilience and developing a cyber resilience framework to form guidelines that the AFI member states, Air Navigation Services Providers and organizations can adopt to effectively uphold cyber resilience in AFI Region.

This document addresses the protection and resilience of Air Navigation Services' critical infrastructure against cyber threats.
It contains general guidelines on how to assess the cybersecurity risks, threats and vulnerability to the aviation systems and operations and methods of mitigating such risks.

The document provides high-level guidelines and practices rather than detailed technical specifications and is based on proven cybersecurity standard and frameworks, and ICAO cybersecurity strategy and guidance material.

This framework is intended to serve as a guide to help AFI member states, Air Navigation Services Providers (ANSP) and organizations be able to develop and align cyber resilience policies, processes, procedures, and controls to protect their systems and operations against cyber threats that would impact confidentiality, Integrity and availability of their services.

Table of contents

Tables of figures

List of Acronyms

Acronym	Definition
ADS-B	Automatic Dependent Surveillance Broadcast
ADS-C	Automatic Dependent Surveillance Contract
AFTN	Aeronautical Fixed Telecommunications Network
AMHS	ATS Message Handling System
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ASECNA	Agency for Aerial Navigation Safety in Africa and Madagascar
ATC	Air Traffic Control
ATM	Air Traffic Management
ATNS	Air Traffic and Navigation Services SOC Limited
ATS	Air Traffic Services
BYOD	Bring Your Own Device.
CNS	Communication Navigation and Surveillance
CPDLC	Controller Pilot Data Link Communications
DoS	Denial of Service
FANS	Future Air Navigation Systems
DDoS	Distributed Denial of Service
FANS	Future Air Navigation Systems
IATA	International Air Transport Association
IoT	Internet of Thing
IP	Internet Protocol
ISMS	Information Security Information Systems
ISO	International Organisation for Standardisation
IT	Information Technology

Definitions

Note. — The explanations given below are to facilitate the understanding of the terms in the context of their use in this document.

Cybersecurity
The body of technologies, controls and measures, and processes and practices designed to ensure confidentiality, integrity, availability and overall protection of systems, networks, programmes, devices, information and data from attack, damage, unauthorized access, use and/or exploitation.

Cybersecurity Policy
A cybersecurity policy documents the intentions and direction of an organization, for the management of cybersecurity threats, as expressed by top management. It is a written document in an organization outlining how to protect the organization from cybersecurity threats, and how to handle incidents and events when they do occur.

Event
Identified occurrence in a system, service or network state indicating a possible breach of information security policy or failures of control, or a previously unknown situation that may be security relevant [ISO/IEC 27035]. It shall be noted that 'occurrence' needs to be considered in its broad sense and shall not be understood as (safety) occurrence term that only embraces the events which have, or could have, significance in the context of aviation safety.

Incident
Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27035-1]

Information Security
Preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved. [BS ISO/IEC 27000:2018]

Information Sharing
The process through which information is provided by one entity to one or more other entities to facilitate risk-based decision-making and promote best practices.

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 Cybersecurity Action Plan]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat entity. This may be a system which directly or indirectly supports a function of the aviation system. [ICAO Cybersecurity Action Plan]

Chapter 1: Introduction

1.1 Background

1.1.1 Cybersecurity is a growing concern for civil aviation, as organizations increasingly rely on commercially available information technology, shared network and computing infrastructure and the public internet for critical parts of their operations, including safety-critical functions.

1.1.2 Cyber-based threats are rapidly evolving and may put air navigation services systems at risk for compromise. The reduction of cyber vulnerabilities and associated risks is critical to improve the resilience of the global aviation system.

1.1.3 Therefore, cybersecurity and cyber resilience are considered by the International Civil Aviation Organization (ICAO) to be emerging and urgent issues in the civil aviation.

ICAO addressed this emerging threat to civil aviation through resolutions A39-19 and A40-10 “addressing cybersecurity in civil aviation”. It is vital that the civil aviation sector integrates cybersecurity policies as part of their normal procedures and integrates them in every part of their aviation system.

1.1.4 Effective information security reduces these risks by protecting the Air Navigation Services against threats and vulnerabilities, and then reduces impacts to its assets. It also assures management and other stakeholders that the organization’s assets and services are reasonably safe and protected against harm, therefore acting as a business enabler.

1.1.5 Within this context, the APIRG IIM Subgroup tasked IIM COM 5 project to develop a comprehensive, strategic framework to reduce and mitigate cybersecurity risks to Air Navigation Services in the Region.

1.1.6 The APIRG IIM Subgroup Project n°5’s aim is to develop an Air Navigation Services cyber resilience framework that will assist the member organizations to effectively:

a) Define and understand their Information Security Requirements;
b) Establish Cyber resilience policies, processes, plans and programs;
c) Implement and operate controls to manage the cybersecurity risks;
d) Monitor and review the performance and effectiveness of the cyber resilience policies; and
e) Continually improve their cybersecurity/cyber resilience based on performance measurements .

1.2 Scope

1.2.1 This framework provides best practices and guidelines for consideration when establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the cyber resilience posture in the context of the organization's overall business risks.

1.2.2 The guidelines and best practices in the framework are standard, generic and vendor neutral.

1.2.3 The framework is intended for Air Navigation Service Provider (ANSP), organizations and civil aviation authorities in the AFI region irrespective of the size and services provided.

1.2.4 This document covers all aviation stakeholders such as Civil Aviation Authorities, Air Navigation Service Providers, Airports operators and any other aviation organization that is part of the State Aviation System.

1.3 Structure of the document

1.3.1

Table *1* below briefly describes the main chapters of this framework.

Chapter	Brief description of content
Chapter 1	Provides the purpose and scope of the documents, the definitions of terms and the structure of the document
Chapter 2	Provides an overview of cyber threats /potential cyber-attackers
Chapter 3	Gives guidelines on asset management
Chapter 4	Provides guidelines on risk management
Chapter 5	Gives guidelines on cybersecurity/ Cyber resilience training and awareness
Chapter 6	Provides useful information on Detection of cyber attacks
Chapter 7	Explains how to respond to a cyber attack
Chapter 8	Gives guidelines on recovery measures.
	References

Table 1 : Structure of the document

Chapter 2: Understanding Cyber threats in Civil Aviation

2.1 Cybersecurity in civil aviation

2.1.1 A national responsibility

2.1.1.1. Aviation security is a national responsibility. In this regard Annex 17 (3.1.1) provides that *"States shall establish and implement a written national civil aviation security programme to safeguard civil aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights."*

2.1.1.2 In the framework of their National Civil Aviation Security Programme it is recommended to States (Annex 17- 4.9.1 & 4.9.2) "**to ensure that appropriate measures are developed in order to protect the confidentiality, integrity and availability of critical information and communications technology systems** and **data used for civil aviation purposes from interference that may jeopardize the safety of civil aviation and** to encourage entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme to **identify their critical information and communications technology systems and data**, including threats and vulnerabilities thereto, and to develop and implement protective measures to include, inter alia, **security by design**, **supply chain security**, **network separation**, and **remote access control**, as appropriate."

2.1.2 ICAO Work on aviation cybersecurity

2.1.2.1 Assembly Resolution A39-19 instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure (Resolution A40-10 – Addressing Cybersecurity in Civil Aviation, superseding Resolution A39-19).

2.1.2.2 ICAO is focused on establishing appropriate mechanisms to mitigate and reduce risks to aviation critical infrastructure from unlawful interference through cyber vectors and from any event that may impact the safety of operations.

2.1.2.3 Secretariat Study Group on Cybersecurity (SSGC) developed the Cybersecurity Strategy endorsed by the ICAO 40th Assembly in 2019.

2.1.3 ICAO Aviation Cybersecurity Strategy[1]

2.1.3.1 The ICAO Aviation Cybersecurity Strategy provides States with a vision of the civil aviation sector as resilient to cyber-attacks, whilst continuing to innovate and grow and to shape a cybersecurity framework, this Action Plan has been developed.

2.1.3.2 The aim of the Strategy is:

- to protect civil aviation and the travelling public from cybersecurity threats.
- to maintain or improve the safety and security of the aviation system in preserving the continuity of air transport services.
- to coordinate cybersecurity measures among State authorities
- to ensure effective and efficient management of cybersecurity risks

2.1.3.3 Seven Pillars of the aviation cybersecurity Strategy

The Aviation Cybersecurity Strategy's seven pillars[2], are:

1. International cooperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity Policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training, and cybersecurity culture.

Figure 1 : Aviation Cybersecurity Strategy's seven pillars

[1] Aviation Cybersecurity Strategy
[2] Aviation Cybersecurity Strategy

2.2 Cyber Threats

2.2.1 The global air navigation services (ANS), airport infrastructure and information systems (**Figure 2**) are exposed to a variety of threat sources, including organized crime, motivated activists also known as called 'hacktivists', state actors, insider threats and accidental or inadvertent system damage due to employee or contractor misuse (**Figure 4**).

2.2.2 Each of these threats can cause a large and widespread disturbance to the order of air and ground operations.

AIRPORT

Figure 2 : Aviation Cyber-threats landscape - Main potential targets in aviation

2.2.3 Two categories of possible cyber threats to Aviation can be distinguished:

Figure 3 : Categories of possible cyber threats in civil aviation

2.3 Threat Actors

2.3.1 Generally, the threat actors are people and groups that engage in attacks on organization network infrastructures with or without malicious intent. **Figure 4** provides an overview of the potential threat actors.

Figure 4 : Potential Cyber threats actors

2.3.2 The motivation for attacking networks/organization can be financial gain, corporate- or state-sponsored espionage, terrorism activities, activism, or simply malicious intent.

2.3.3 The action of threat actors can result in loss of confidentiality, compromise of integrity or loss of availability of an organization system.

2.4 Cyber threats landscape

2.4.1 A cyber threat can be defined as "any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority.[3]"

2.4.2 The cyber threats landscape is large and evolves rapidly. **Figure 5** shows the top 8 cyber prime threats groups encountered within the time period July 2021 to July 2022, identified in the ENISA[4] Threat Landscape 2022 (issued in October 2022).

Figure 5 : Eight (8) top threats (that have dominated the threat landscape in 2022) – source: ENISA Threat Landscape Report 2022

2.4.3 According to the ENISA Transport Threat Landscape 2022[5], the "aviation sector is facing multiple threats, with data-related threats being the most prominent, coupled by ransomware and malware[6]. "In 2022, there has been a rise in the number of ransomware attacks affecting airports. Fraudulent websites impersonating airlines have become a significant threat in 2022."[7]

[3] CANSO Cyber Security and Risk Assessment Guide (definition source: US Department of Homeland Security)
[4] European Union Agency for Network and Information Security - https://etl.enisa.europa.eu/#/
[5] https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape
[6] "Customer data of airlines and proprietary information of original equipment manufacturers (OEM) are the prime targeted assets of the sector". (source : ENISA Transport landscape, issued march 21, 2023
[7] https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

2.4.4 Air Traffic management (ATM), Communication, Navigation and Surveillances system (CNS), Information Management (IM) and other important systems for aviation are exposed to many different types of cyber threats which can be intentional or unintentional[8], targeted or non-targeted (as shown on **Figure 6**).

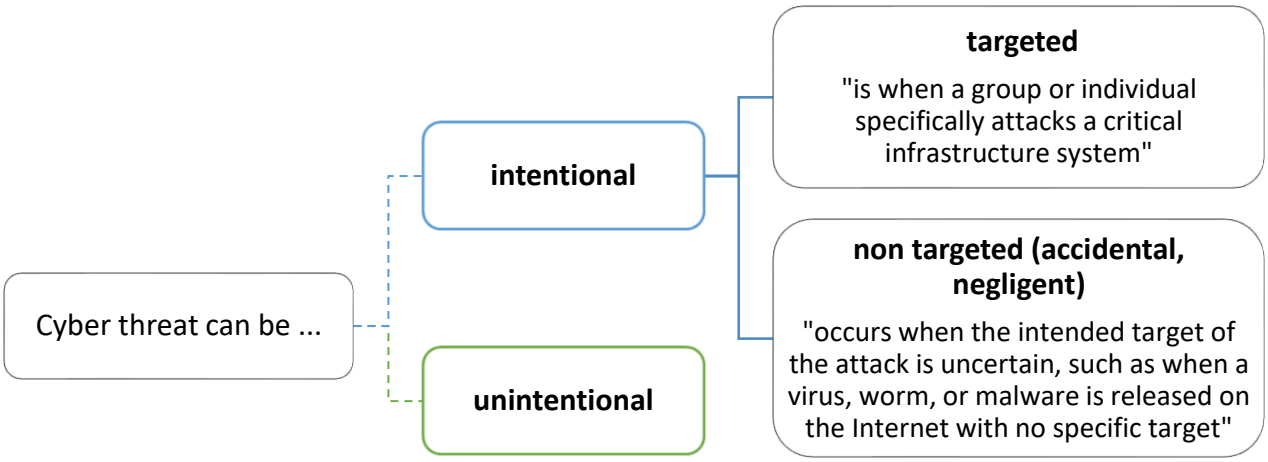

Figure 6: Types of cyber threats

2.5 Cybersecurity attack Vectors

2.5.1 The deployment of different cyber threats can be done using one or more attack vectors.

2.5.2 The list below provides some predominant attacks vectors[9] :

[8] Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures and equipment failures that inadvertently disrupt computer systems or corrupt data.

[9] ENISA report provides a categorization of the most predominant and noteworthy attack vectors observed by ENISA throughout the year (2018)

Figure 7: various types of cyber threats vectors

2.6 Air Navigation Services Critical Systems

2.5.1 The critical Information systems in Air Navigation Services that are susceptible to cybersecurity threats include (as depicted in figure 8):

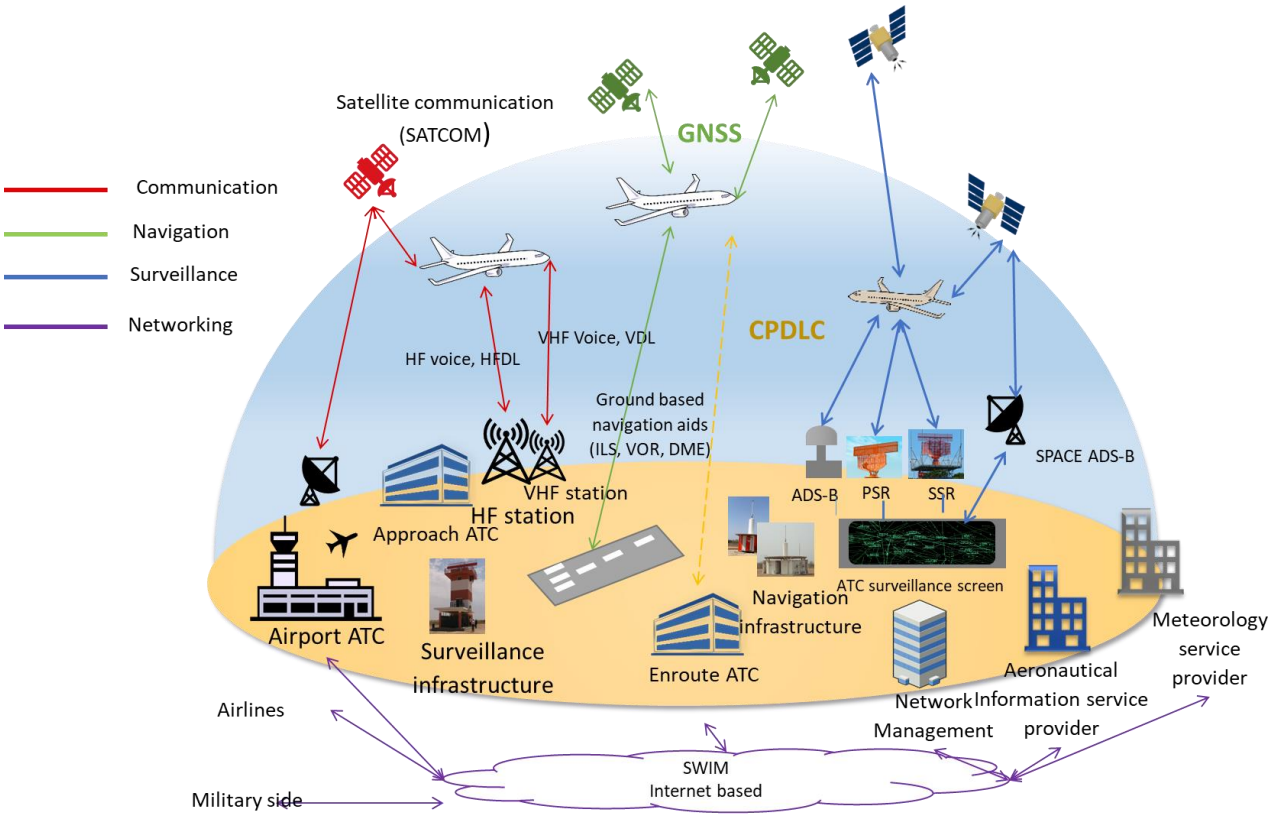

Figure 8: Overview of the various critical infrastructure in air navigation facilities[10]

1. CNS/ATM Systems	a) Flight Data Processor (FDP) b) Aeronautical Fixed Telecommunications Network (AFTN) c) HF & VHF Communication systems d) Global Navigation Surveillance Systems (GNSS) e) Air-Ground Data Link systems f) ADS-B Systems (terrestrial, Space ADS-B) g) ADS-C Systems h) Aeronautical Billing Systems i) FANS/CPDLC Systems j) Satellite Communication (SATCOM) Systems
2. Networking and Other Supporting IT systems	a) Email Communication systems b) Active Directory Systems c) Light Weight Directory Access Protocol systems d) Domain Name Systems (DNS) e) Web and Database Servers
3. Aeronautical Information Management systems	a) ATS Message Handling System (AMHS)

[10] A. A. Elmarady, K. Rahouma: Studying Cybersecurity in Civil Aviation, October 28, 2021.

4. Aeronautical Meteorological System	a) Satellite Distribution System (SADIS)

2.5.2 "Aeronautical systems are vulnerable to cyber threats such as:

- IT sabotage,
- data corruption and availability (notably ransomware),
- software corruption, communication disruption or interruption,
- satellite communication interference,
- cyber-attacks including systems sabotage,
- data breaches, damage, and destruction of hardware"[11].

2.5.3 The cyber threat landscape "may materialise in the form of possible attack scenarios against the integrity and availability of ANS data, networks, and systems, with an impact on safety, capacity and service continuity, e.g.,"[12].:

- Denial of service by jamming or spoofing CNS signals, data, or systems, e.g., surveillance data processing systems, data link communications or GPS.
- Corruption of CNS data integrity;
- corrupting, through false instructions or information;
- ADS-B false-aircraft transmissions – so-called falsedata injection attack;
- attacking key infrastructure element such as SWIM (system wide information).

2.5.4 The following figure provides few examples of cyber-attacks, among many others, on the above listed ANS critical systems.

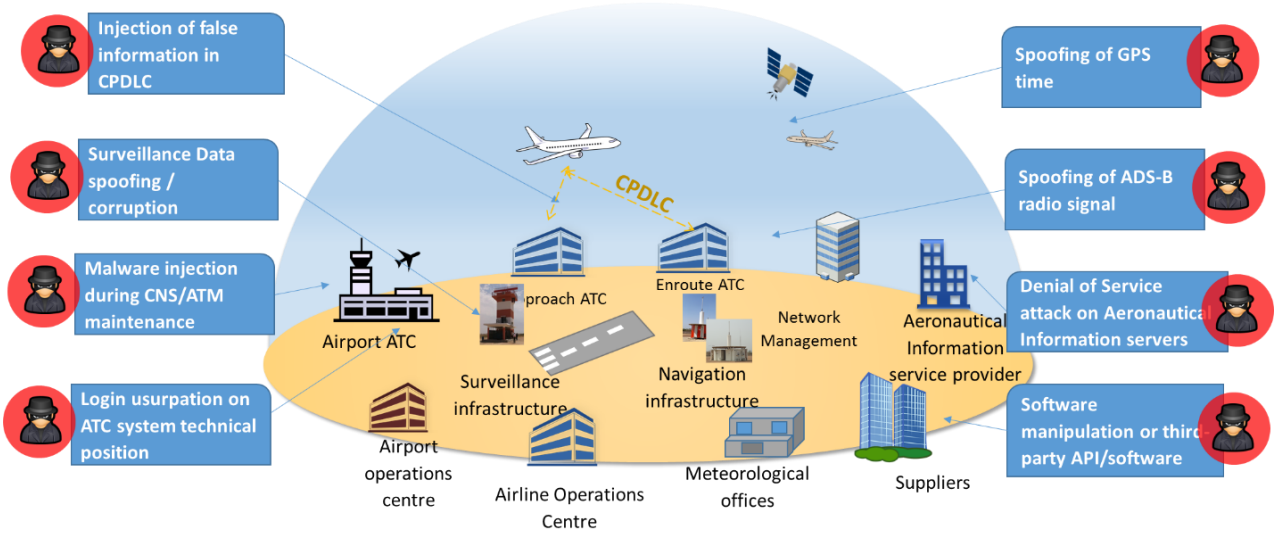

Figure 9 : examples of possible cyber-attacks on ANS critical systems

[11] Air Traffic Management Cybersecurity Policy Template

[12] https://www.unitingaviation.com/strategic-objective/security-facilitation/air-traffic-management-security-genesis-evolution-and-future-challenges/

2.5.5 In a recent paper titled "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment," the authors M. Ahmed Abdelwahab Elmarady and Kamel Rahouma provide a list of potential cyber threats in various "critical infrastructure in aviation systems, such as air-ground communication, radio navigation aids, aeronautical surveillance, and system-wide information management (SWIM)."

The following table lists potential cyber threats in various air navigation services critical systems:

ANS critical system		Threat type/ attack scenario
Air-ground[13] communication protocols	**VHF voice**	- Eavesdropping[14] - Jamming (unintentional radio interference due to use of unlicensed frequencies) - Jamming (unauthorized access to block the VHF frequencies) - Spoofing (unauthorized access to send fake instructions between ATC and pilot)
	CPDLC	- Eavesdropping (listening to the data traffic messages) - Jamming (Channel blocking) - Flooding (transmitting multiple packets of CPDLC data to the same receiving entity) - Injection (sending, possibly faulty, unauthorized messages) - Alteration (modification of message content) - Masquerading (attacker impersonates an authorized user whether ghost aircraft or ATC)
	ACARS	- ACARS weight / balance update and the ACARS flight plan update events
Radio navigation aids	**Satellite – based navigation**	- Unintentional interference - Intentional interference - Spoofing
	ILS	- Single-tone attack - Overshadow attack
	VOR	- Jamming - Spoofing
Aeronautical surveillance technique	**SSR**	- Jamming - Spoofing - Over-interrogation
	MLAT	- Miss synchronization due to vulnerabilities in GPS
	ADS-B	- Eavesdropping - Jamming - Spoofing

Table 2 : Potential cyber threats in various air navigation services critical systems

[13] A. A. Elmarady, K. Rahouma: Studying Cybersecurity in Civil Aviation

[14] An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices. Source : www.fortinet.com

2.7 Common Cybersecurity Vulnerabilities

2.7.1 In Information security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.

2.7.2 Some common Cybersecurity vulnerabilities in Air Traffic management are listed below:

2.8 Establishing Cybersecurity Policy

Note: The International Civil Aviation Organization (ICAO) develops a model Cybersecurity Policy for reference by Member States and industry when developing their own national/internal policies[15].

2.8.1 Organizations should define the scope of their Information Security Requirements considering their location, assets, and technology in use.

2.8.2 The organizations shall set objectives and desired state of the cybersecurity within their institutions.

2.8.3 The Cybersecurity Policy will help to focus resources and actions to achieve a systemic approach to cybersecurity within the organization.

[15] ICAO Cybersecurity Policy Guidance

Chapter 3: Asset Management

3.1 Asset Management

3.1.1 General

3.1.1.1 The objective of asset management is to actively manage all organization's hardware devices and software applications on their network so that only authorized devices are given access to the authorized users whereas the unauthorized devices can be identified and prevented from gaining access, and unauthorized software applications are prevented from installation and execution.

3.1.1.2 An asset can be defined as Anything of value to the organization that must be protected including servers, infrastructure devices, end devices and data.

3.1.1.3 Asset management should consider beyond the traditional hardware and software in the Network. New technologies should be given attention to. These include BYOD, cloud applications and infrastructure, virtualization, mobile devices, IoT Devices.

3.1.1.4 Assets are subject to both deliberate and accidental threats while the related processes, systems, networks, and people have inherent vulnerabilities.

3.2 Critical Infrastructure

3.2.1 Air Navigation Services Providers' assets should be classified as critical infrastructure. Critical Infrastructures (CIs) are defined as ICT systems that are essential for the operation of critical infrastructures/assets such as telecommunications, computers/software, internet, satellites, etc.

Chapter 4: Risk Assessment and Management

4.1 Background

4.1.1 All aviation stakeholders should:

- "Implement a cyber security risk management regime that includes continuous identification and assessment of cyber risks, mitigation of vulnerabilities, robust governance structures and risk ownership.
- Ensure that cyber risks are managed throughout the lifespan of any new and developing systems, platforms, and technologies."

4.1.2 Risk Assessment and Management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the assets from cybersecurity threats. The cybersecurity risk management should be a continual process that define the risks, assess the risks, and formulate plans, processes, and activities to mitigate the risks.

4.1.3 The cybersecurity risk management is intended to contribute the following:

1. Be able to identify the risks
2. Be able to assess the risks against their consequences to the operations and the likelihood of their occurrence
3. Be able to effectively communicate the identified risks and likelihood to the stakeholders and understood by all stakeholders
4. Establish of risk mitigation measures
5. Establish priority for actions to reduce the risks
6. Establish knowledge management tools to capture, monitor and improve risk management processes
7. Build the capacity of staff and all stakeholders about the risks and actions to take to mitigate them.

4.2 Risk Management

4.2.1 Risk management defines countermeasures i.e., solutions to protect and mitigate a threat or risk, and outline the impact / damage that the threat will cause to the organization impacted by the breach:

4.2.2 The objectives of risk assessment are to identify risks, quantify the risks, qualitatively describe the risks, prioritize the risks against evaluation criteria and the organization's objectives.

4.2.3 The processes involved in risk management are listed in the figure below:

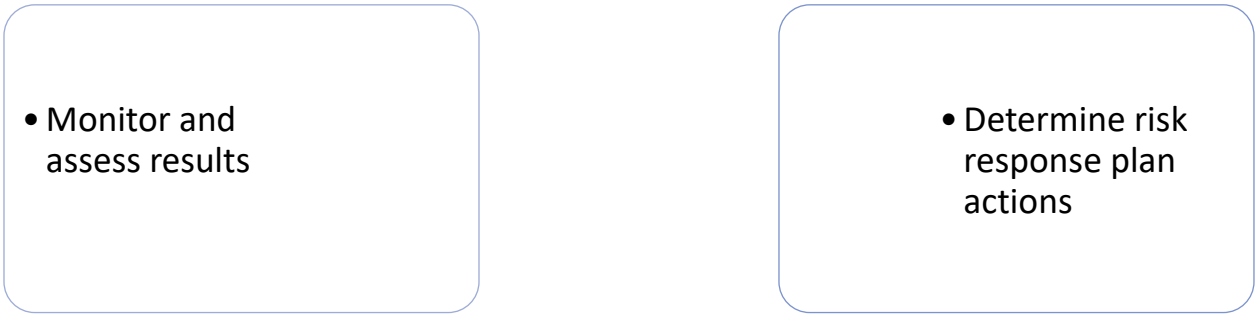

Figure 10 : Risk management processes

4.2.3 Potential consequences of cybersecurity breach may include:

a) Loss of trust from clients / airspace users
b) Loss of confidentiality e.g., Information leakage to unauthorized individuals
c) Loss of Information Integrity e.g., Altered / Corrupted information such as Flight Plans
d) Loss of System Access / Availability because of DDoS attacks

Chapter 5: Cybersecurity culture

5.1 Introduction

5.1.1 "A positive cybersecurity culture 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."[16]

*Note: The **ICAO "Cybersecurity Culture in Civil Aviation"** provides States and industry with guidance on designing and implementing cybersecurity culture in civil aviation".*

5.1.2 "Cybersecurity culture should be endorsed by organizational leadership and should include a programme to be undertaken by all personnel[17].

5.1.3 "Cybersecurity culture should include elements from safety and security cultures, e.g., self-reporting, reporting of suspicious behaviour/practice, just culture, etc"[18].

5.1.4 A robust and effective cybersecurity culture in civil aviation is based on the following core elements[19]:

[1]. leadership;
[2]. cross-domain links;
[3]. communication;
[4]. awareness, training and education;
[5]. reporting systems;
[6]. continuous review and improvement; and g) positive work environment.

These seven core elements of a strong cybersecurity culture are depicted in the figure below :

[16] ICAO Cybersecurity Culture in Civil Aviation – guidance – January 2022
[17] Cybersecurity Policy Guidance, January 2022
18 Cybersecurity Policy Guidance; §4.9.3 - January 2022
[19] ICAO Cybersecurity Culture in Civil Aviation – guidance – January 2022

Figure 11 : Strong Cybersecurity culture seven core elements[20]

5.2 Cybersecurity awareness and training

5.2.1 Introduction

5.2.1.1 The Cybersecurity culture programme should include recurrent cybersecurity education (including principles of cyber hygiene practices), awareness on latest threats, training, and testing (both as part of training and live simulation of attacks) to assess the level of cyber awareness/hygiene.

5.2.1.2 The capacity building, training and cyber security culture is considered as one of the main pillars to enable having cyber resilient aviation system during normal and crises times. Therefore, ICAO resolution for cyber security should consider this critical issue. Furthermore, the new established cyber security panel should consider also this issue in their tasks.

5.2.1.3 Training and awareness are key elements of Cyber resilience. A broad cybersecurity/Cyber resilience awareness and training should be implemented by the AFI stakeholders to enhance the ability of their personnel to recognize the diverse

[20] ICAO Cybersecurity culture in civil aviation – January 2022

range of cyber threats and their capability to critically impact upon Air Navigation Services and daily operations.

5.2.1.3 Employees are AFI stakeholders' first and primary line of defence against cyber-attacks.

5.2.2 Cybersecurity learning continuum

5.2.2.1 "Learning is a continuum"[21], starting with awareness, building to training, and evolving into education (**Erreur ! Source du renvoi introuvable.**).

5.2.2.2 Cybersecurity learning needs[22] should be identified for:

- distinct roles within the organization (ANSPs, CAA, airlines, ...),
- all civil aviation personnel who interact with the organization's digital assets and
- different responsibilities in relation to organization's IT systems, as depicted on Figure 12.

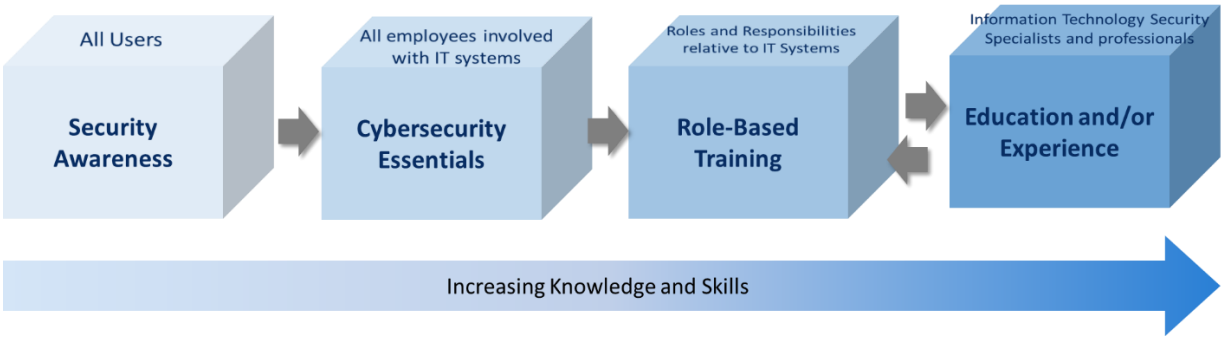

Figure 12 : IT Security learning continuum model (NIST)[23]

5.2.3 Pillars of Cybersecurity/Cyber resilience awareness and training

5.2.3.1 The key pillars of cybersecurity awareness and training are depicted in the figure below:

[21] Information Technology Security - Training Requirements: A Role-and Performance-Based Model. NIST Special Publication 800-16
[22] The IT learning model is role-based:
[23] Information Technology Security Training Requirements – NIST - NIST Special Publication 800-16

Figure 13 : Cyber security and resilience awareness and training pillars

5.2.3.2 Cybersecurity awareness shall be provided to all AFI Stakeholders personnel and partners (subcontractors, suppliers …)[24].

5.2.3.3 The personnel shall be trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

5.2.3.4 Aviation Cyber threats landscape evolves rapidly, and various vulnerabilities may appear. Therefore, cybersecurity / cyber resilience awareness and training should be repetitive, updated and constantly tested.

5.3 Reporting Systems

5.3.1 Organizations should develop and implement of an internal cybersecurity reporting system[25].

5.3.2 Reporting systems allow the organization "to:

- proactively manage its cyber risks,
- measure the development of the organization's cybersecurity posture,
- identify and plan awareness and training needs of staff, and
- adapt its internal processes, controls, and measures in line with the development of cybersecurity trends and with the maturity of cybersecurity culture."[26]

5.3.3 "Cybersecurity reporting systems gather elements from both aviation safety and aviation security reporting systems. They address both:

[24] NIST SP 800-53 Rev. 4 AT-2, PM-13
[25] Cybersecurity culture in civil aviation, 1st edition – ICAO – January 2022
[26] Cybersecurity culture in civil aviation, 1st edition – January 2022

- reporting of self-actions/errors that are not in line with the organizational information security policies and processes,
- reporting of suspicious/erroneous behaviour of other employees”

Chapter 6: Detection

6.1 Introduction

6.1.1 Cyber resilience is a measure of how well aviation stakeholders can operate their business during a data breach or cyber-attack.

Cyber resilience pillars are depicted in ***Figure 14*** below:

Figure 14: Cyber resilience pillars [1]

6.1.2 Detection in this instance refers to proactive monitoring of critical infrastructure within Air Navigation Services Systems.

6.2 Detection

6.2.1 The Detect pillar focuses on developing and implementing the appropriate activities to monitor cyber events to rapidly identify an attack; manage events to assess the systems that may be affected, and to develop processes, procedures and plans to ensure a timely response to potential cyber-attacks.

6.2.2 The Detect pillar as identified in ***Figure 14*** above and will address the following elements (listed in the table below):

Security Monitoring

Table 3 **Adapted from NIST Framework - Detect Stage [2]**

Chapter 7: Response

7.1 Introduction

7.1.1 Cybersecurity incident response is defined as the development and implementation of appropriate end-to-end cyber security incident management process of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

7.1.2 Cybersecurity incident response processes are underpinned by policies and procedures, defined roles and responsibilities, appropriate equipment, infrastructure, tools, and supporting materials ready, and qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way (NIST 2014, Haufe et al. 2016, and Killcrece 2005).

7.1.3 To effectively manage security and incidents, cross-functional computer security incident response teams (CSIRT) are required to effectively manage and execute cyber security incidents plans and processes.

A computer security incident response team (CSIRT) is an organization that aims to provide information security incident response services to a particular community.

7.1.4 Cyber security incident response frameworks such as National Institute of Standards and Technology (NIST) and European Network and Information Security Agency (ENISA) developed standards and recommendations as baseline for organisations to manage cyber security incidents.

The frameworks provide guidelines on how to identify critical infrastructure, protect and secure identified assets, detect anomalies and events through continuous monitoring, respond to cyber-attacks through communication and information sharing, and lastly, to restore and recover affected critical assets (NIST 2017, ENISA 2015).

Figure below, depicts incident response process/model.

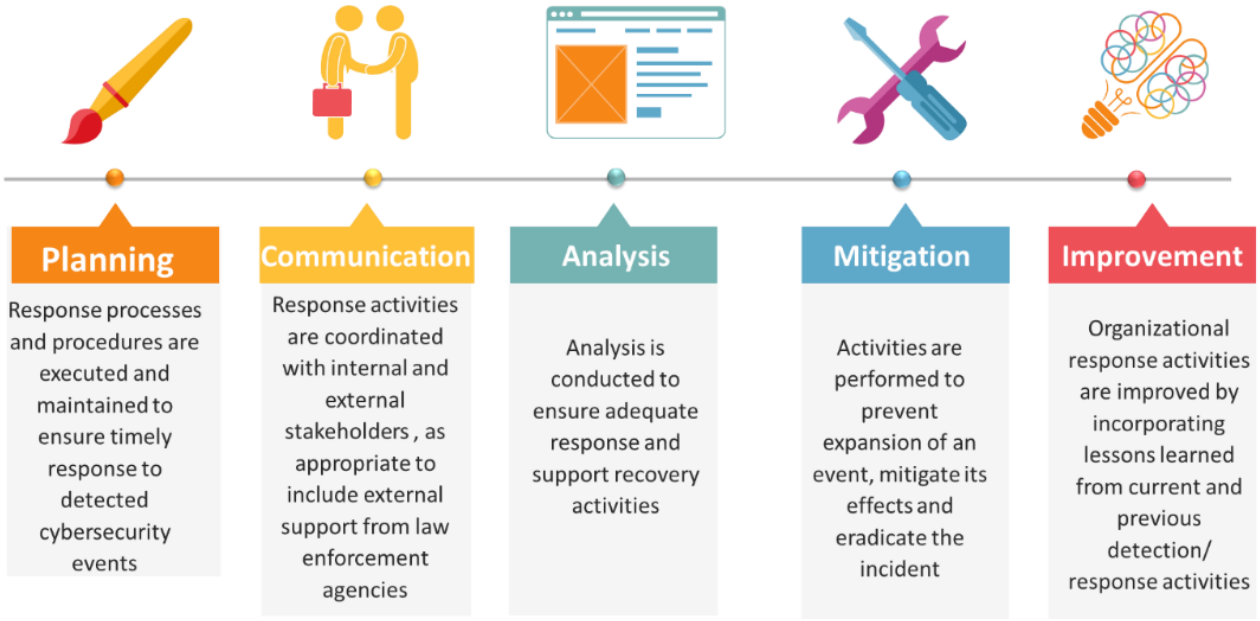

Figure 15 : **Incident response process adapted from the NIST framework**[27]

7.2 Incident response stakeholders

7.2.1 To operate an effective global air transportation system, aviation industry partners need to collaborate and share information through an integrated ICT platform. Collaboration of ICT systems allows aviation stakeholders to collate and distribute planning and flight progress information, distribute event predictions and status messages, generate advisories and alerts.

7.2.2 Interoperability is achieved globally through exchange of common information exchange models and services.

7.3 Digital forensics to identify threat actors

7.4 Incident response policies, procedures, and plans

7.4.1 COBIT 5, CSC-18, NIST SP 800, ISO/IEC 27001:2013, and ISO/IEC TR 18044 best practice standards support the implementation of an integrated cyber security incident response plan.

7.4.2 Cyber security incidents plans must be integrated to security related capabilities to enable stakeholders to better manage their cybersecurity risk posture and reduced information security incidents.

7.4.3 "Testing emergency response and business continuity plans should be periodically conducted with the aim to improve the plans as well as the capabilities of responders. Testing should include all relevant stakeholders and comprise a combination of Tabletop Exercises (TTX) as well as live tests."[28]

[27] NIST framework incident response process
[28] ICAO Cybersecurity Policy Guidance – January 2022

Chapter 8: Recovery

8.1 Introduction

8.1.1 Recovery relates to restoring any capabilities or services that were impaired due to a cyber-event.

8.1.2 In this regard, each aviation stakeholder will document appropriate recovery activities and methods, a lessons-learned process for continuous improvement and a recovery communication plan for users and other stakeholders [1].

8.2 Recovery process

8.2.1 "Organizations should develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident"[29].

8.2.2 The **Recover** process supports timely recovery to normal operations to reduce the impact from a cybersecurity incident (Recovery Planning; Improvements; and Communications).

8.2.3 The figure below describes the recovery process from NIST, which includes recovery Planning, Improvement, and communication.

Figure 16: Recovery process adapted from the NIST framework [2]

[29] NIST

CONCLUSION

Cyber resilience is key factor in the aviation sector that should be considered by all aviation industry stakeholders.

As Aviation will never be 100% cyber proof[30], there is a need to be prepared to cyber events. Proactive, collective and coordinated African wide response shall be adopted. This Cyber resilience framework provided in this document is an initial step.

The establishment of a pan –African Air Navigation Services cyber resilience framework is the only way forward addressing the following :

Policies, plans and guidance material

a) Provisions for cyber security, including identification of threats and risks, capability, and capacity development, shall be developed at a regional and national level.

b) Policies to protect ATM/CNS infrastructure/systems shall be developed. This policy should include State's responsibility for their protection, their provision operation and monitoring and Penalties for cyber-attacks.

Awareness, training, and capacity building

c) Cyber awareness training for all stakeholder staff and management. CAA and Operators should train their technical personnel in cybersecurity.

d) Massive and continuous sensitization of aviation stakeholders on the importance of cyber resilience shall be conducted.

e) CNS and ATM systems awareness training shall be provided to IT technicians training in case of cyber-attack.

Coordination mechanisms

f) Collaboration and exchange of information between States shall be defined.

g) Comprehensive and timely information sharing will help mitigate the risks.

h) Trusted information sharing through a secured platform.

African Civil Aviation Authorities Adequate Cyber Resilience Oversight capabilities

i) Development by CAAs of cyber resilience requirements and build capacity in terms of employing or training cyber resilience analysts who will oversee proper implementation of cyber resilience by ANSPs.

j) Frequent IT Security Audit of all parties that connect to ANSP should be conducted.

[30] [28] Eurocontrol Aviation Intelligence Think paper n°3 – Cyber security in Aviation.

k) States oversight encompassing cyber resilience of their CNS/ATM systems and drills/simulations.

Responses to cyber attacks

l) ANSP (or any aviation stakeholder) shall establish Security Operations Center (SOC) to monitor, protect, detect, respond, and recover from cyber threats and attacks.

m) There is a need to implement a task-team at both the National and Regional levels that will come up with workable solutions to cyber safety and resilience threats.

n) Nomination of PoC for cyber safety and resilient

o) Simulations/drills to assess the effective implementation of the policy.

Normative References

1. ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements*

2. ISO/IEC 27002:2015 *Information technology — Security techniques —Code of Practice for Information security management systems*

3. ISO/IEC 27005:2018 *Information technology - Security techniques - Information security risk management.*

4. National Institute of Standards and Technology - *Framework for Improving Critical Infrastructure Cybersecurity* Ver 1: 2018

5. ICAO Annex 10 - *Aeronautical Telecommunications*

6. ICAO Annex 17 - *Security*

References

Title	Edition, date
[1]. Aviation Cybersecurity Strategy - ICAO	October 2019
[2]. Cybersecurity Policy Guidance	January 2022
[3]. ICAO Cybersecurity Action Plan	Second edition January 2022
[4]. Cybersecurity Culture in Civil Aviation	1st edition January 2022
[5]. Assembly Resolution A39-19	
[6]. Resolution A40-10 – Addressing Cybersecurity in Civil Aviation, superseding Resolution A39-19	
[7]. Annex 17 — Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference to the Convention on International Aviation	
[8]. Doc 9750, Global Air Navigation Plan 5th Edition	
[9]. Doc. 9854, Global Air Traffic Management Operational Concept	
[10]. Doc 9855, Guidelines on the Use of the Public Internet for Aeronautical Applications	
[11]. Dubai Declaration on cybersecurity in Civil Aviation	
[12]. Using Traffic Light Protocol	
[13]. CANSO guidance material (Standard of excellence in Cybersecurity, ATM Cybersecurity Template)	
[14]. Air traffic management cybersecurity policy template – Latin America and the Caribbean	
[15]. EUROCONTROL EATM-CERT 1st Quarter 2022 Cyber Threat Landscape & Activity Report for Senior Management	
[16]. Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment- Authors: AHMED ABDELWAHAB ELMARADY 1 AND KAMEL RAHOUMA	date of current version October 28, 2021.
[17]. "The Connectivity Challenge: Protecting Critical Assets in a Networked World – A Framework for Aviation Cybersecurity", The American Institute of Aeronautics and Astronautics (AIAA).	August 2013
[18]. ENISA Threat Landscape 2021	2021
[19]. UK Aviation Cybersecurity https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf	
[20]. Symantec Corporation, "The Cyber Resilience Blueprint : A New Perspective on Security," 2014.	

Title	Edition, date
[21]. T. Grance, K. Kent, and B. Kim, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ.*, vol. 800–61, p. 79, 2012.	
[22]. ICAO EUROPE, Middle East, and Africa (EMEA) Cybersecurity in Civil Aviation Summit, Bucarest, Romania, 7 to 9 May 2018 – Outcomes and conclusions	
[23]. Bucharest Communique – Recommendations for a cybersecurity strategy in International Civil Aviation Bucharest, Romania 7 to 9 May 2018	9 May 2018
[24]. CIVIL AVIATION CYBERSECURITY INFORMATION REPOSITORY https://www.icao.int/cybersecurity/Pages/default.aspx	
[25]. CONVENTION on the Suppression of Unlawful Acts Relating to International Civil Aviation	Beijing, 10 September 2010
[26]. Civil Aviation Cybersecurity Action Plan (ICAO, CANSO, IATA, ASD, ICCAIA, ACI) **https://www.icao.int/cybersecurity/SiteAssets/ICAO/Civil%20Aviation%20Cybersecurity%20Action%20Plan%20-%20SIGNED.pdf**	05 December 2014
[27]. Information Paper WP 160 - THIRTEENTH AIR NAVIGATION CONFERENCE - Montréal, Canada, 9 to 19 October 2018 -CONSIDERATIONS ABOUT CYBERSECURITY IN AVIATION (Presented by Austria on behalf of the European Union and its Member States, the other Member States of the European Civil Aviation Conference and by EUROCONTROL)	
[28]. Eurocontrol Aviation Intelligence Unit Think Paper #3 - Cyber Security in aviation	August 2019
[29]. The Cyber Security Oversight Process for Aviation - CAP 1753 – UK Civil Aviation Authority	December 2019
[30]. GAMMA project, - Global ATM Security Management Project European Union's Seventh research and innovation Framework Programme. http://www.gamma-project.eu.	2017
[31]. ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS	JULY 2022
[32]. ENISA THREAT LANDSCAPE: TRANSPORT SECTOR (January 2021 to October 2022)	MARCH 2023