Civil-Military Considerations for SWIM Deployment

Interoperability in SWIM Deployment

Edition: 1.0
Edition date: 14/04/2025
Classification: white

EUROCONTROL

DOCUMENT CONTROL

Document Title	Civil-Military Considerations for SWIM Deployment
Document Subtitle	Interoperability in SWIM Deployment
Document Reference	This field is automatically updated
Edition Number	1.0
Edition Validity Date	31-12-2026
Classification	White
Status	Final
Author(s)	Jaroslaw Kwasniewski (CNSS)
Contact Person(s)	Jaroslaw Kwasniewski (CNSS)

APPROVAL TABLE

Authority	Date	Signature
Prepared by:	14/04/2025	
Reviewed and endorsed by:	08/05/2025	
Approved by:	08/05/2025	

EDITION HISTORY

Edition No.	Validity Date	Author(s)	Reason
1.0	31/12/2026	Jaroslaw Kwasniewski	Final

TABLE OF CONTENT

1. EXECUTIVE SUMMARY 2
2. INTRODUCTION 2
3. SCOPE 2
4. BACKGROUND AND ASSUMPTIONS 2
5. SWIM ARCHITECTURE AND COMPONENTS 3
6. SECURITY CONSIDERATIONS 4
6.1. Confidentiality, Integrity and Availability (CIA) 4
6.2. Sensitivity of data 5
6.3. Access Control and Identity Management 5
6.4. Data Transmission and Storage 6
6.5. Deployment 6
6.5.1. Cybersecurity Framework 6
6.5.2. Cyber-Resilience 6
7. INTEROPERABILITY REQUIREMENTS 7
7.1. SWIM Service Interoperability 7
7.2. Information Exchange Models 7
7.3. Technical Infrastructure Requirements 9
8. GOVERNANCE AND COMPLIANCE 9
9. SWIM TECHNICAL INFRASTRUCTURE 9
10. ICAO DEVELOPMENTS 12
11. NATO POSITION ON SWIM 13
12. RECOMMENDATIONS FOR MILITARY ORGANIZATIONS 13
13. CONCLUSION 14

TABLE OF FIGURES

Figure 1 SWIM Architecture 4
Figure 2 Representation of an example FIXM data 8

TABLE OF TABLES

Table 1 - Abbreviations table 16

1. Executive Summary

This document serves as a guide to integrating civil and military considerations for the deployment of System Wide Information Management (SWIM). It addresses the security and interoperability requirements necessary for military systems to participate effectively in SWIM. The aim is to provide a structured framework to ensure that military systems can securely and efficiently exchange not sensitive air traffic management (ATM) information with civil counterparts, thereby enhancing overall ATM capabilities.

2. Introduction

The deployment of System Wide Information Management (SWIM) marks a significant evolution in how information is managed and shared within Air Traffic Management (ATM). SWIM facilitates enhanced situational awareness and operational coordination by enabling seamless data exchange across different systems and stakeholders, including civil and military entities. This document outlines the key security and interoperability considerations essential for integrating military systems into the SWIM environment. By adhering to these guidelines, military organizations can ensure secure and interoperable participation in SWIM, contributing to the safety, efficiency, and resilience of air traffic management.

3. Scope

This document is intended to provide guidance and support for military organizations in implementing the security and interoperability requirements of SWIM [1][2][3]. The focus is on ensuring that military systems can seamlessly integrate into the SWIM environment while maintaining high standards of security and operational efficiency. The guidance applies to SWIM services, information exchanges, and technical infrastructure.

4. Background and Assumptions

System Wide Information Management (SWIM) is designed to improve information sharing within the ATM network. Military integration into SWIM presents unique challenges and opportunities, given the distinct nature of military operations and the sensitivity of military data. This document is based on the following assumptions:

- Military organizations will have varying roles within SWIM, potentially as both providers and consumers of information services.

- The integration of military systems into SWIM requires careful consideration of security requirements to protect sensitive information.

- Effective governance and compliance with standards [1][2][3] are essential for the successful deployment of SWIM.

5. SWIM Architecture and Components

System Wide Information Management (SWIM) is structured around a Service-Oriented Architecture (SOA) that enables the integration of diverse ATM systems. The key components of SWIM include:

- SWIM Information: This component involves the standardization of data definitions and exchange formats to ensure consistency and reliability in information sharing. SWIM information standards such as AIXM (Aeronautical Information Exchange Model) and FIXM (Flight Information Exchange Model) play a critical role in facilitating interoperability.

- SWIM Information Services: SWIM provides a range of services that manage the provision and consumption of information across various ATM domains. These services include data publication, subscription, request, and response mechanisms that facilitate efficient information exchange.

- SWIM Technical Infrastructure (SWIM-TI): The technical infrastructure supports the secure and reliable exchange of information. SWIM-TI includes messaging protocols, network configurations, and security mechanisms that underpin SWIM operations.

- SWIM Governance: Governance is essential to ensure that SWIM operates within defined parameters, with clear policies and procedures for managing security, conformance to requirements, and interoperability. SWIM governance structures must include representation from both civil and military stakeholders to address the diverse needs of the ATM community.

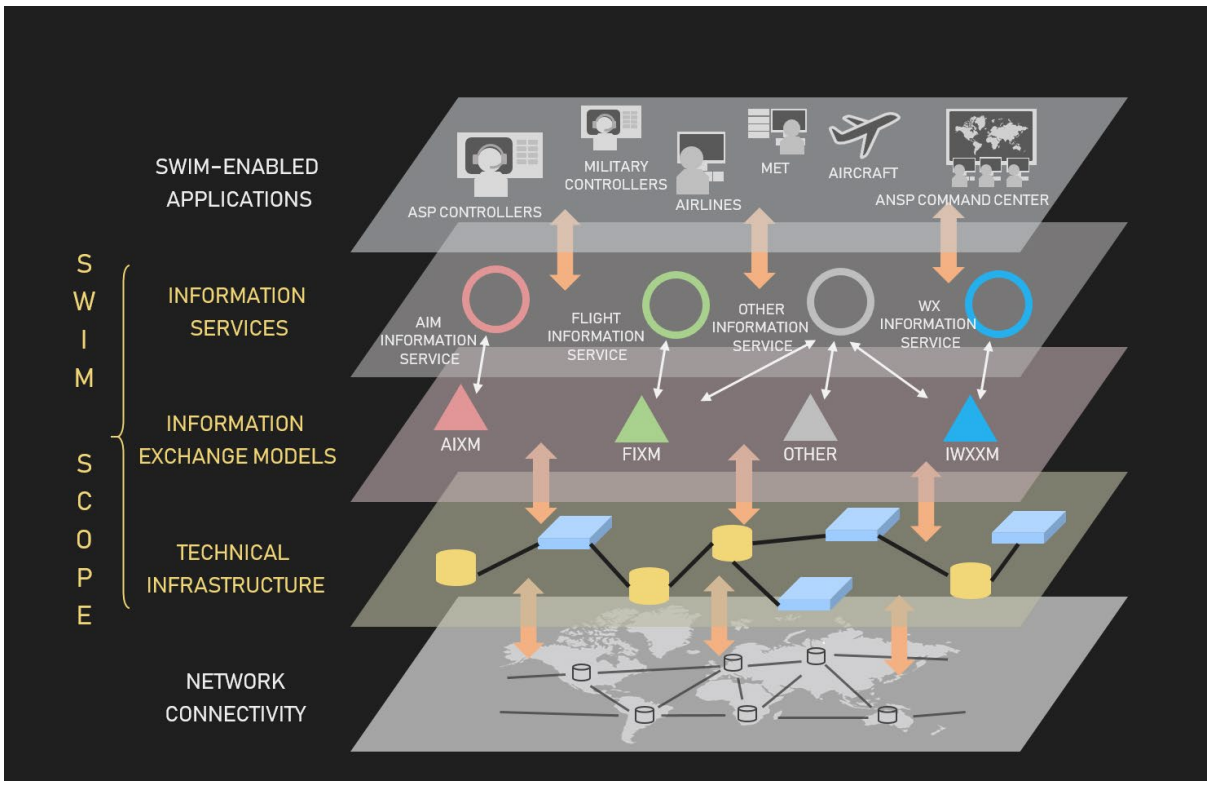

Figure 1 SWIM Architecture

6. Security Considerations

Security is a paramount concern in the deployment of SWIM, particularly given the sensitivity of military data and the potential risks associated with cyber threats. This section outlines the key security considerations for SWIM deployment, focusing on confidentiality, integrity, availability, data classification, access control, and secure data transmission and storage.

6.1. Confidentiality, Integrity and Availability (CIA)

The security of SWIM is grounded in the principles of confidentiality, integrity, and availability [5]:

- Confidentiality: Data must be protected against unauthorized access to ensure that information is not disclosed to unauthorized parties. SWIM implements encryption and access control measures to maintain data confidentiality.

- Integrity: The integrity of data must be preserved to prevent unauthorized alterations that could compromise the accuracy and reliability of information. SWIM implements for verifying data integrity, such as cryptographic hash functions and digital signatures.

- Availability: The availability of data is critical to ensure that authorized users can access the information they need when they need it. SWIM is designed to provide high availability, with redundancy and failover mechanisms to prevent disruptions.

When discussing data confidentiality within the context of SWIM, it is important to note that confidentiality is not being addressed in traditional military terms of classification. Instead, confidentiality here refers to ensuring that access to information is restricted to authorized users only, protecting data from unauthorized disclosure or access, regardless of its classification level.

6.2. Sensitivity of data

Generally, data classification involves categorizing information to determine the necessary security measures, ensuring that sensitive data is properly protected. However, SWIM is not intended to process any classified data in the military context.

Sensitive data refers to information that requires protection due to its confidential, personal, or strategic nature. There is currently no universally accepted definition of what constitutes sensitive data, leading to variations in interpretation and implementation across different organizations and systems. As a result, the identification and handling of sensitive data may vary, making it crucial to establish clear guidelines and criteria specific to the operational context and stakeholder requirements.

6.3. Access Control and Identity Management

Effective access control is essential to prevent unauthorized access to military data within SWIM. Access control policies should be based on the principle of 'need-to-know,' ensuring that only authorized individuals can access specific information. Key components of access control include:

- Authentication: SWIM can implement robust authentication mechanisms, such as multi-factor authentication (MFA) and Public Key Infrastructure (PKI), to verify the identity of users accessing sensitive data.

- Authorization: Authorization mechanisms should be used to enforce access control policies, ensuring that users have the necessary permissions to access specific data. Role-based access control (RBAC) can be used to manage access based on users' roles and responsibilities.

- Identity Management: Identity management systems should be integrated into SWIM to manage user identities and access rights. This includes the use of digital certificates, identity providers, and federated identity management to facilitate secure access across different systems.

6.4. Data Transmission and Storage

The secure transmission and storage of data are critical components of SWIM security:

- Data Transmission: Sensitive military data need to be transmitted over secure channels, such as NewPENS (New Pan-European Network Services) [9.4, 9.5] or through individual Virtual Private Networks (VPNs) with encryption protocols, using crypto devices and security equipment and software (e.g. data diode, boundary protection devices). In contrast, non-sensitive data can be transmitted over the internet using secure HTTP (HTTPS) with appropriate encryption measures.

- Data Storage: Sensitive data cannot be stored on portable devices or in external cloud services. Storage systems must be equipped with robust access controls, data encryption, and integrity verification mechanisms to prevent unauthorized access and data tampering. Storage equipment should be Tempest[1] or at least fallow the physical secure rules (e.g. distance from other electronic equipment or wires).

6.5. Deployment

Cybersecurity is a critical aspect of SWIM deployment, given the increasing reliance on interconnected ICT systems and the potential risks posed by cyber threats.

6.5.1. Cybersecurity Framework

A comprehensive cybersecurity framework is essential to protect SWIM from cyber threats. Key elements of the cybersecurity framework include:

- Security Controls: SWIM allows to implement a range of security controls to protect against cyber threats. This includes network firewalls, intrusion detection systems (IDS), encryption, and access controls and could also include data diode or boundary protection devices (BPD).

- Threat Monitoring: SWIM deployment should include continuous monitoring for potential threats and vulnerabilities. This involves using security information and event management (SIEM) systems to detect and respond to security incidents.

- Incident Response: deployed SWIM solutions should have a robust incident response plan in place to address security breaches. This includes procedures for detecting, containing, and mitigating incidents, as well as communication protocols for notifying stakeholders.

6.5.2. Cyber-Resilience

Cyber-resilience refers to the ability of SWIM to withstand and recover from cyber incidents. Key elements of cyber-resilience include:

[1]TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) refers to the susceptibility of computer and telecommunications devices to data theft. Some electronic equipment emits electromagnetic radiation or compromising emanations in a manner that can be used to reconstruct intelligible data.

- Prevention: Implementing preventive measures to reduce the likelihood of cyber incidents. This includes regular security and risk assessments, vulnerability scans, and security awareness education & training.

- Preparedness: Developing and maintaining contingency plans to ensure that SWIM can continue to operate during a cyber incident. This includes defining roles and responsibilities, establishing communication protocols, and conducting regular drills.

- Response and Recovery: Implementing procedures for responding to and recovering from cyber incidents. This includes activating incident response teams, isolating affected systems, and restoring normal operations as quickly as possible.

7. Interoperability Requirements

Interoperability is a key objective of SWIM, enabling seamless information exchange across different ATM systems. This section outlines the interoperability requirements for SWIM, focusing on service interoperability, information exchange models, and technical infrastructure requirements.

7.1. SWIM Service Interoperability

SWIM's service-oriented architecture facilitates interoperability by enabling systems to interact through standardized services. Key considerations for SWIM service interoperability include:

- Standard Service Descriptions: SWIM services are described using standard formats and protocols to ensure compatibility between different systems. Service descriptions include information on service interfaces, message formats, and data models.

- Service Discovery: SWIM provides mechanisms for service discovery, allowing systems to find and access services dynamically. This is achieved through the use of service registries that catalogue available services and provide metadata for service discovery.

- Service Interaction Patterns: SWIM supports various interaction patterns, including request/reply (R/R), publish/subscribe (P/S), and notification-based interactions. These patterns facilitate different types of information exchange, enabling systems to interact in a flexible and efficient manner.

7.2. Information Exchange Models

Standardized information exchange models are essential for achieving interoperability in SWIM. Key information exchange models relevant to SWIM include:

- Aeronautical Information Exchange Model (AIXM): AIXM provides a standard framework for the exchange of aeronautical information, including airspace structure, airport data, and navigation aids. Military systems participating in SWIM should conform to AIXM standards to ensure consistent information exchange.

- Flight Information Exchange Model (FIXM): FIXM is used for exchanging flight-related information, such as flight plans, clearances, and flight status updates. Military systems should adopt FIXM standards to facilitate the exchange of flight information with civil ATM systems.

- Weather Information Exchange Model (WXXM): WXXM provides a standard format for exchanging weather information, which is critical for flight planning and operations. SWIM participants should use WXXM to ensure the interoperability of weather data across different systems.

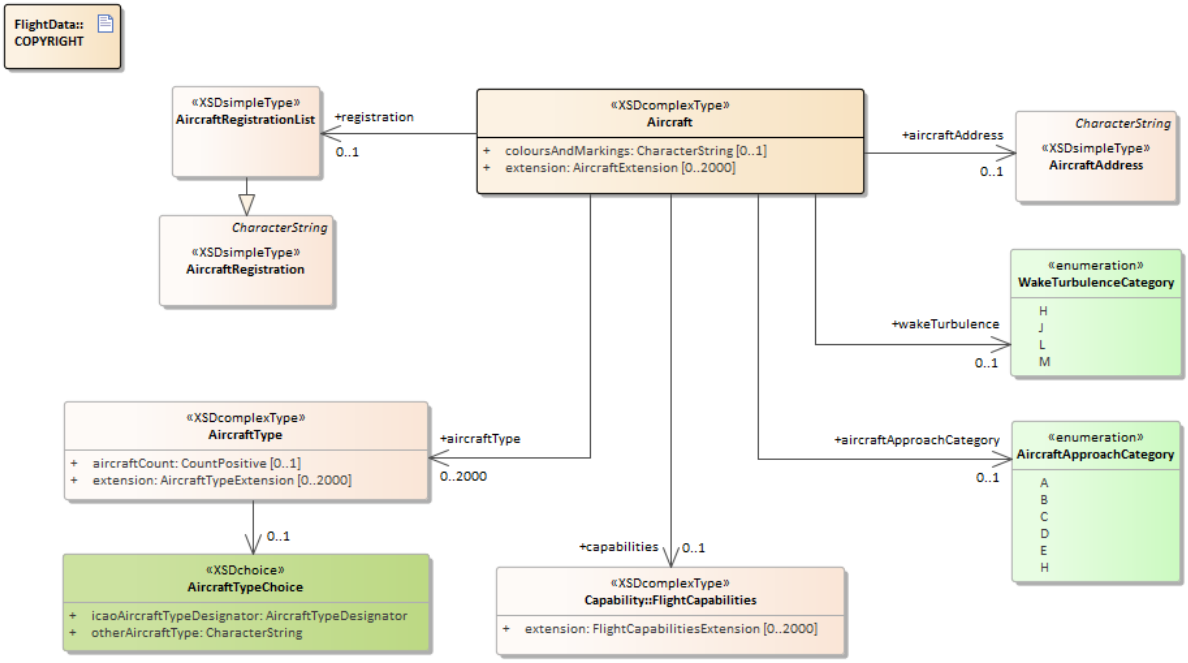

Figure 2 Representation of an example FIXM data

7.3. Technical Infrastructure Requirements

The SWIM Technical Infrastructure (SWIM-TI) provides a robust and secure foundation for information exchange. Key features of SWIM-TI include:

- Messaging Protocols: SWIM-TI supports standard messaging protocols, such as REST or AMQP (Advanced Message Queuing Protocol).

- Network Interface Bindings: SWIM-TI includes standard network interface bindings that support different types of network configurations, including IP-based networks and virtual private networks. This enables SWIM to operate across various network environments.

- Quality of Service (QoS): SWIM-TI supports QoS mechanisms to ensure that information exchange meets the required performance standards, managing bandwidth, latency, and reliability to meet the needs of different stakeholders.

8. Governance and Compliance

Effective governance is essential for the successful deployment of SWIM. Governance structures include representation from both civil and military stakeholders to address the diverse needs of the ATM community. Key governance considerations include:

- Policy Development: Governance bodies develop policies that define the rules and standards for SWIM operations. This includes policies on security, data sharing, and interoperability.

- Compliance Monitoring: SWIM governance includes mechanisms for monitoring compliance with established policies and standards. This contains conducting regular audits, security assessments (risk and vulnerabilities), and reviews to ensure that SWIM operations adhere to defined requirements.

- Stakeholder Engagement: Governance structures facilitate active engagement with stakeholders, including civil aviation authorities, military organizations, and industry partners. This ensures that all parties have a voice in SWIM development and deployment.

9. SWIM Technical Infrastructure

The System Wide Information Management (SWIM) Technical Infrastructure (TI) provides the necessary framework for secure, efficient, and reliable communication between various stakeholders in the aviation industry, including air traffic management (ATM), airlines, airports, and meteorological services.

9.1. Key Components of SWIM Technical Infrastructure

- The messaging capabilities of SWIM TI facilitate the exchange of information through various communication patterns such as publish/subscribe and request/reply. These capabilities ensure that the right information is delivered to the right stakeholders at the right time, enhancing situational awareness and decision-making processes.

- Security is paramount in the aviation sector, and SWIM TI incorporates robust security measures to protect information integrity and confidentiality. This includes identity access management, digital certificates, and encryption technologies to safeguard data against unauthorized access and cyber threats.

- Effective management of the technical infrastructure is crucial for maintaining high performance and reliability. SWIM TI includes tools for monitoring system performance, detecting faults, and ensuring seamless operation. These management capabilities help in proactively addressing issues and maintaining the overall health of the information exchange network.

9.2. Implementation and Standards

The implementation of SWIM TI is guided by a set of international standards and protocols to ensure interoperability and consistency across different systems and regions. These standards are developed by organizations such as the International Civil Aviation Organization (ICAO) , the European Organisation for the Safety of Air Navigation (Eurocontrol), European Union Aviation Safety Agency (EASA) and European Organisation for Civil Aviation Equipment EUROCAE.

9.3. Challenges and Future Directions

While SWIM TI offers numerous benefits, its implementation also presents challenges such as the need for significant investment in infrastructure, the complexity of integrating legacy systems, and ensuring global interoperability. Future developments in SWIM TI will focus on addressing these challenges and leveraging emerging technologies such as artificial intelligence and machine learning to further enhance information management capabilities.

9.4. NewPENS Architecture

NewPENS (New pan-European Network Services) is the primary network infrastructure supporting SWIM. Key features of NewPENS include:

- MPLS and VRF Technologies: NewPENS uses Multi-Protocol Label Switching (MPLS) and Virtual Routing and Forwarding (VRF) technologies to create secure virtual private networks (VPNs) for different stakeholders. This allows for the segmentation of network traffic and enhances security.

- Service Delivery Points (SDP): NewPENS includes Service Delivery Points (SDPs) that provide connectivity between the network and stakeholder systems. SDPs are monitored for security and performance, ensuring reliable communication.

- Network-to-Network Interface (NNI): NewPENS can interface with other networks through Network-to-Network Interfaces (NNIs). This allows for secure data exchange between different network environments.

9.5. Security in NewPENS

While NewPENS provides a secure environment for data exchange, additional security measures are required to protect sensitive military data. Key security considerations for NewPENS include:

- Encryption: Data transmitted over NewPENS should be encrypted to protect against unauthorized access. This includes using PKI-based encryption for sensitive data.

- Firewall and Intrusion Detection: Stakeholders should implement firewalls and intrusion detection systems at their premises to protect against unauthorized access and cyber threats.

- Monitoring and Logging: NewPENS includes monitoring and logging capabilities to detect and respond to security incidents. Security Operation Centres (SOC) monitor network activity and respond to potential threats. Computer Security Incident Response Teams (CSIRTs) react, act in response to a security incident once it has been detected

10. ICAO Developments

The International Civil Aviation Organization (ICAO) plays a critical role in shaping global cybersecurity standards for aviation. This section outlines key ICAO initiatives related to SWIM and cybersecurity.

10.1. ICAO Cybersecurity Strategy

ICAO's Aviation Cybersecurity Strategy outlines a comprehensive approach to enhancing cybersecurity resilience in the aviation sector. Key elements of the strategy include:

- International Cooperation: ICAO promotes international cooperation to address cybersecurity challenges. This includes sharing information on threats, vulnerabilities, and best practices.

- Governance: ICAO emphasizes the importance of effective governance structures to oversee cybersecurity efforts. This includes developing policies, standards, and guidelines for cybersecurity.

- Capacity Building: ICAO supports capacity-building initiatives to enhance cybersecurity capabilities within the aviation sector. This includes training programs, workshops, and technical assistance.

10.2. Security Considerations in the ICAO Manual

The ICAO Manual on System Wide Information Management (SWIM) provides guidance on security considerations for SWIM deployment. Key security aspects addressed in the manual include:

- Information Security: The manual emphasizes the importance of protecting information from unauthorized access, disclosure, and alteration. This includes implementing encryption, access controls, and data integrity measures.

- Cybersecurity: The manual outlines the need for a comprehensive cybersecurity framework to protect SWIM from cyber threats. This includes implementing security controls, threat monitoring, and incident response procedures.

- Resilience: The manual highlights the importance of resilience in SWIM, ensuring that systems can continue to operate during and after a cyber incident. This includes developing contingency plans and recovery procedures.

11. NATO position on SWIM

The utilization of SWIM (System Wide Information Management) Services is seen as a key enabler for enhancing situational awareness. Allies using SWIM Services can provide and consume advanced Meteorology (MET) and Space Weather (SWX) services, promoting civil-military interoperability and cooperation. An effective CNS (Communication, Navigation, and Surveillance) strategy will ensure NATO's CNS network adapts to the specific profiles and protocols required for SWIM, without compromising security and defense activities. Allies are encouraged to support SWIM to enhance situational awareness and data sharing with military and civilian ATM (Air Traffic Management) organizations. However, integration should not impact NATO's operational capabilities in degraded or contested environments, and resilience must be maintained, and sensitive data must be preserved and protected. Non-SWIM compliant military ATM and air defense organizations should be accommodated through conventional networking structures.

12. Recommendations for Military Organizations

To ensure the secure and effective integration of military systems into SWIM, the following recommendations are provided:

- Implement Comprehensive Security Policies: Military organizations should develop and enforce security policies that align with SWIM requirements to protect sensitive data.

- Enhance Access Control: Implement robust MFA authentication and authorization mechanisms to control access to sensitive information.

- Conduct Regular Security (risk and vulnerabilities) Assessments: Perform periodic security risk assessments to identify vulnerabilities and implement necessary mitigations.

- Engage in SWIM Governance: Actively participate in SWIM governance activities to influence policies and ensure military interests are represented.

- Invest in Education & Training and Awareness: Provide regular cybersecurity training for personnel involved in SWIM operations to enhance awareness and preparedness.

13. Conclusion

The deployment of SWIM presents significant opportunities for enhancing civil-military cooperation in air traffic management. By addressing the security and interoperability requirements outlined in this document, military organizations can ensure their successful integration into the SWIM framework, contributing to a safer, more efficient, and resilient air traffic management environment.

References

[1] EUROCONTROL Specification for SWIM Technical Infrastructure Yellow Profile, Ed. 1.1, 5 July 2020

[2] EUROCONTROL Specification for SWIM Service Definition Ed. 1.0, 12 April 2024

[3] EUROCONTROL Specification for SWIM Information Definition Ed, 1.0., 1 December 2017

[4] ICAO Aviation Cybersecurity Strategy, October 2019

[5] ICAO Air Traffic Management Security Manual, Doc 9985

Abbreviations (Optional)

Term	Definition
AIXM	Aeronautical Information Exchange Model
AMQP	Advanced Message Queuing Protocol
ATM	Air Traffic Management
CIA	Confidentiality, Integrity, Availability
FIXM	Flight Information Exchange Model
ICAO	International Civil Aviation Organization
MET	Meteorology
MPLS	Multi-Protocol Label Switching
PENS	Pan-European Network Services
PKI	Public Key Infrastructure
REST	Representational State Transfer
SWIM	System Wide Information Management
SWX	Space Weather
VRF	Virtual Routing and Forwarding

Table 1 - Abbreviations table

SUPPORTING
EUROPEAN
AVIATION