EUROCONTROL

SWIM CYBERSECURITY HINTS & TIPS

Practical guidance material
for secure SWIM implementation

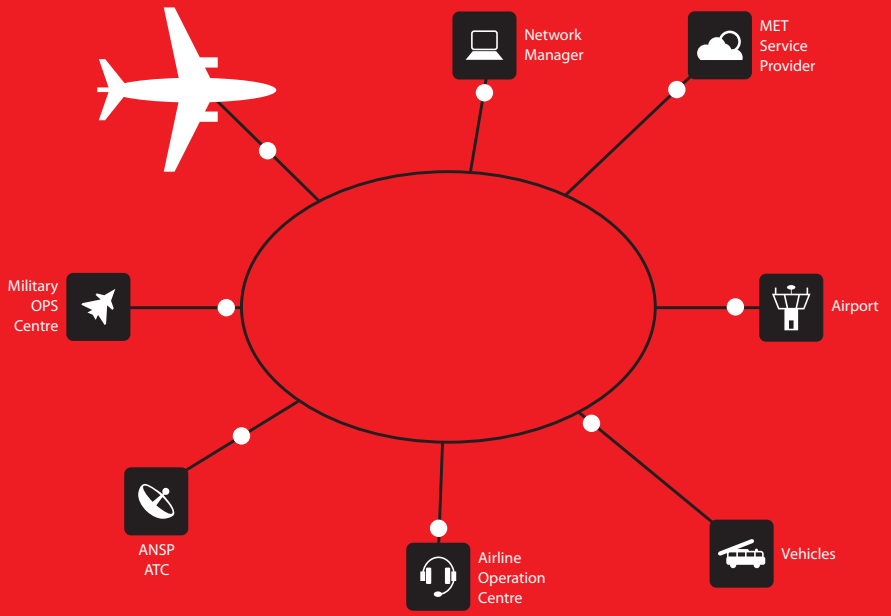
INTRO

INTRODUCTION

SWIM is modernising ATM. More information is being shared by stakeholders that are increasingly interconnected and dependent on information communication technologies (ICT). This makes for more efficient ATM operations but also increases the risk of cyber-attacks.

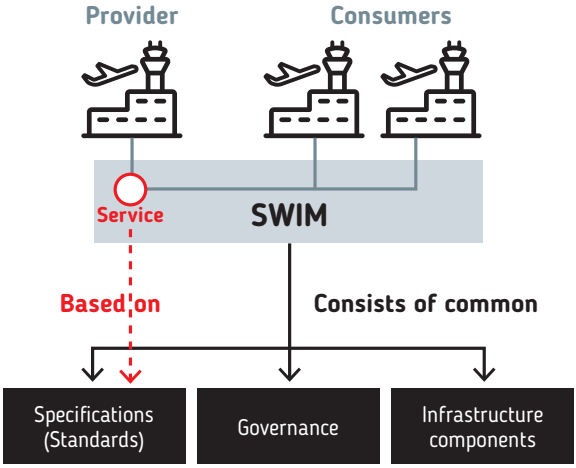
Cybersecurity in SWIM has to be addressed on several levels, including governance and common infrastructure components. It absolutely has to be an integral part of SWIM system specifications and methods.

This brochure gives SWIM implementers an overview of the most important security aspects to consider. It is intended for use as guidance for self-assessment only: it is not a means of compliance or a substitute for an exhaustive security methodology.



SWIM

System Wide Information Management (SWIM) is a far-reaching development in Air Traffic Management (ATM), changing how information is managed and shared by stakeholders. SWIM supports ATM operational activities by enabling the secured exchange of aeronautical, flight, meteorological, air traffic flow and surveillance information.



SWIM definition

SWIM: the definition

As defined by ICAO, SWIM consists of standards, infrastructure and governance to facilitate the management of ATM-related information and its exchange between qualified parties through interoperable services.

SWIM: the scope

SWIM aims at improving interoperability in ATM using widely adopted technologies, standards and best practices (e.g. AIXM, Internet Protocol, Web Services, Service Oriented Architecture).

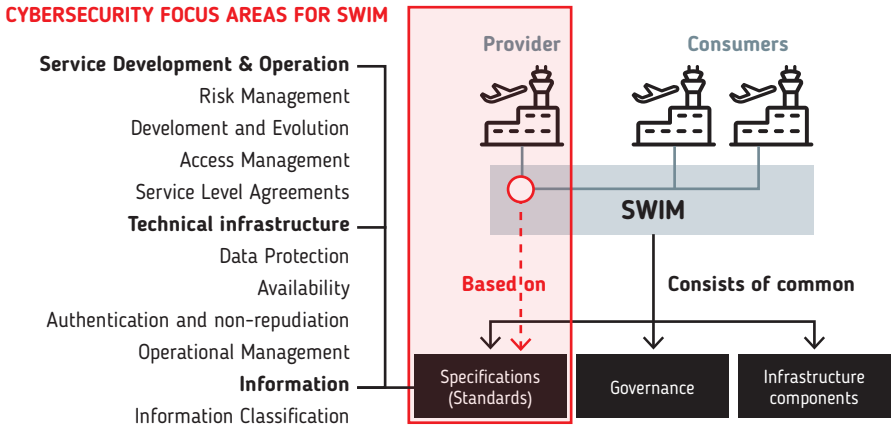
Interoperability in SWIM is achieved by using common specifications for implementing the service interfaces used in exchanging information between ATM stakeholders. The coordinated development of these common specifications is achieved through common governance, undertaken by SWIM stakeholders. Finally, there are common infrastructure components that support SWIM implementation (PKI - Public Key Infrastructure, Service Registry).

SWIM: the implementers

SWIM is implemented primarily through automating organisations' exchange of information (e.g. Flight Plan Filing, Weather Information) through system interfaces. Using these SWIM services enables these organisations (or **service providers**) to interoperate with other organisations which use their services/information (the **service consumers**).

CYBERSECURITY IN SWIM

SWIM underpins better, more efficient decision-making with interoperability standards that facilitate the exchange of information between ATM stakeholders. In consequence, organisations become increasingly interconnected and dependent on the information and communication technology (ICT) that increases their vulnerability to cyber-attacks. So, cybersecurity becomes an aspect of vital importance when implementing SWIM.



Cybersecurity focus areas for SWIM

Cybersecurity: the definition

As described in ICAO's security manual, cybersecurity encompasses those safeguards and actions used to protect the cyber domain from threats that may harm interdependent networks and information infrastructure.

Cybersecurity entails setting up protective controls against the risks inherent in interconnected ICT systems. Threats to the systems may be made intentionally or not; they can affect information, ICT systems or any other dependent ATM asset/activity.

SWIM's cybersecurity scope

This brochure focuses on cybersecurity for SWIM implementation. It is not intended to be an ICT security manual; it highlights elements of cybersecurity that are most relevant when implementing SWIM. Aspects such as ATM operational resilience, contingency and recovery belong to the domain of ATM Security – the overarching term for all security-related aspects in ATM – and are not covered here.

Cybersecurity in SWIM will need to be addressed on multiple levels:

- governance (e.g. common security policy, security coordination activities);
- common infrastructure components (e.g. PKI);
- system specifications and methods used by the entity implementing SWIM.

This brochure focuses on the latter point; it provides practical guidance to take into consideration when implementing SWIM services.

CYBERSECURITY GUIDANCE FOR SWIM

This section provides a set of recommendations based on best practices and standards to mitigate the risk of cyber-attacks in SWIM. The recommendations have been drawn up for SWIM service implementers that need to address security issues during service development and operational phases. Additionally, as services enable the exchange of information and use technical infrastructure, further recommendations are given.

SERVICE DEVELOPMENT & OPERATION

Service Risk Management

- Has a risk management methodology been adopted by the organisation to determine the criticality levels of services and the ICT supporting them?
- Have security events which could interrupt services supporting critical business processes been identified? Have the likelihood of their occurrence and their potential impact/consequences been quantified?
- Is there an inventory on security threats and known vulnerabilities that can be used to support this risk assessment?

Related References:

- NIST SP 800-53r4 Family: Risk Assessment
- ISO/IEC 27001:2013 §6.1.2

Service Development and Evolution

- Has the development lifecycle for services and their underlying ICT systems been defined?
- Is sufficient security documentation for services and their underlying ICT systems available? (e.g. secure configuration, installation and use; known vulnerabilities …)
- Have new/updated services and their underlying ICT systems been tested during development and prior to acceptance, using security criteria?
- Has the data input from applications been validated to ensure correct and appropriate processing by the services?
- Does the acceptance process include the acceptance of security test results and residual risk by the service owner?
- Have development, testing and operational services and their underlying ICT systems been separated to reduce the risks of unauthorised access or changes to the operational system?
- Is training on the correct use and operation of services and their underlying ICT systems provided?

Related References:

- NIST SP 800-53r4 Family: System and Services Acquisition
- ISO/IEC 27002:2013 §14

Service Access Management

- When granting external access to information or services: have the risks been identified? Have appropriate controls been implemented?
- Have access control policies for systems and services been established, documented and reviewed, based on business and access security requirements?
- Is access to information systems based on established access control policies?
- Are security-related events (e.g. login) recorded? Are these logs preserved?
- Are unsuccessful logon attempts monitored and countermeasures defined when a maximum number of attempts is exceeded?
- Are service access sessions terminated after a certain period of inactivity?
- Is there a formal user registration and de-registration procedure in place for granting and revoking access to all services? Is the allocation and use of privileges restricted and controlled?

Related References:

- NIST SP 800-53r4 Family: Access Control
- ISO/IEC 27002:2013 §9

Service Level Agreements

- Do all agreements with third parties involving information or information processing facilities cover the relevant security requirements?
- Is the acceptable use of information assets and services clearly stated?
- Have the requirements for confidentiality or non-disclosure agreements, reflecting the organisation's needs for the protection of information, been identified? Are they regularly reviewed?

Related References:

- NIST SP 800-53r4 Family: System and Services Acquisition
- ISO/IEC 27002:2013 §15

INFORMATION

Information Classification

- Does the organisation maintain an inventory of information assets, their ownership, and their traceability to the services that expose this information to external parties?
- Is there a documented and agreed classification system for information which is used to set protective measures?
- Is there an appropriate set of procedures for information labelling and handling in accordance with the classification scheme?

Related References:

- NIST SP 800-53r4 Family: Security
- ISO/IEC 27002:2013 §8.2

INFRASTRUCTURE

ICT System Protection

- Do the ICT supporting systems define usage quotas for users, processes and services?
- Do the ICT supporting systems have controls and protective measures for different kinds of denial of service attacks?
- Has the ICT support system been protected from unauthorised code execution?
- Are security events detected, recorded and securely stored (e.g. failed authentication requests, protected resources access requests)?
- Are inactive sessions terminated after a predefined amount of time?
- Does the ICT system consist of software components with verified origin, authenticity and integrity?
- Has the ICT system undergone a documented security patching process that protects it against known vulnerabilities in a predefined maximum delay?
- Is the ICT system subject to a documented yearly vulnerability assessment which includes penetration tests?

Related References:

- NIST SP 800-53r4 Family: System and Communications Protection
- ISO/IEC 27002:2013 §13.2.3, 12.6.1

Data Protection

- Has the information input process been validated to ensure that it is consistent with the expected content? (e.g. validation against protocol specifications, message definitions)
- Has the data integrity and origin authentication been protected, using cryptographic methods?
- Are there any controls that will protect the confidentiality of sensitive information exchanges based on encryption?
- Are there suitable back-up arrangements for data including, if appropriate, secure off-site storage?
- Is the system's integrity and confidentiality assured, with sensitive or critical data encrypted?

Related References:

- NIST SP 800-53r4 Family: System and Information Integrity
- ISO/IEC 27002:2013 §10, §13

Authentication, Authorisation and Non-Repudiation

- Is there an authentication policy defining valid security credentials (e.g. password, PKI certificates, tokens …), their lifecycle, strength, issuance and renewal process as well as secure storage and transmission?
- Are users, services and devices uniquely identified by the ICT support systems?
- Are there any controls in place to enable authentication?
- Is role base access control enforced for protected resources?
- Is the use of strong passwords enforced?
- Is the access of entities that surpass a defined number of failed authentication attempts restricted?
- Is access control to any request originating from or with a destination to an external network enforced?

Related References:

- NIST SP 800-53r4 Family: Identification and Authentication
- ISO/IEC 27002:2013 §10, §11

Operational Management

- Is there any protection mechanism in place to prevent tampering or unauthorised access of logs/tools etc.?
- Are detection, prevention and recovery controls in place to protect against malicious code in all systems?
- Does the acceptance process include the acceptance of security test results and residual risk by the system owner?
- Have security patches been obtained and implemented in a timely manner?
- Are development, test, and operational infrastructure systems separated so as to reduce the risks of unauthorised access or changes to the operational system?

Related References:

- NIST SP 800-53r4 Family: Contingency Planning
- ISO/IEC 27002:2013 §14

REFERENCES

These documents were used or referred to in drawing up this paper:

- **ICAO SWIM Concept Manual**

  http://www.icao.int/airnavigation/IMP/Documents/SWIM%20Concept%20V2%20Draft%20with%20DISCLAIMER.pdf

- **ICAO Aviation Security Manual**

  http://www.icao.int/Security/SFP/Pages/SecurityManual.aspx

- **EUROCONTROL Manual for ATM Security Oversight**

  https://www.eurocontrol.int/sites/default/files/publication/files/2012-manual-for-national-atm-security-oversight.pdf

- **EUROCONTROL ICT Guidance (Guidance to ANSPs for practical implementation of ICT security regulatory requirements)**

- **NIST SP 800-53r4 (Security and Privacy Controls for Federal Information Systems and Organisations)**

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- **ISO/IEC 27002:2013 (Information technology – Security techniques – Code of practice for information security management)**

  https://www.iso.org/standard/54533.html

- **ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems - Requirements)**

  https://www.iso.org/standard/54534.html

FOR FURTHER INFORMATION, PLEASE CONTACT:

EUROCONTROL SWIM Unit
e-mail: swim@eurocontrol.int

Produced by EUROCONTROL
Directorate ATM Programmes
96, rue de la Fusée, B-1130 Brussels, Belgium