

SWIM GOVERNANCE «COMMON SECURITY REQUIREMENTS»

SWIM Open Day

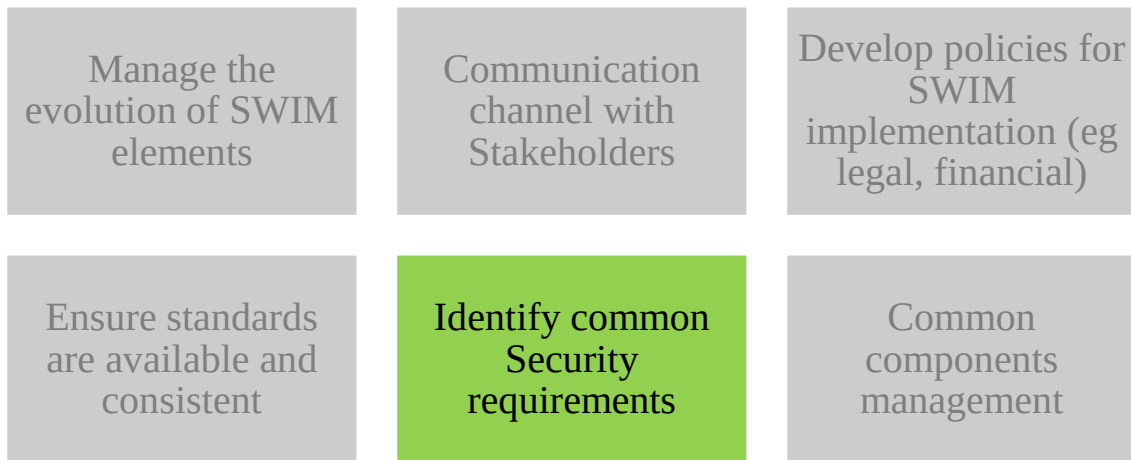


Alessandro Manzo (Techno Sky / ENAV)
Rome, 05/07/2018

Security within the SWIM Governance

The basics: to ensure a stable implementation and controlled evolution of SWIM standards, guidance material, common components, compliance...

→ COMMON SECURITY REQUIREMENTS are part of the «picture»



SWIM Governance WBS



Task 1	Project Management (DSNA)	07/02/2017	01/07/2019
Task 2	Set up SWIM Governance (DFS)	07/02/2017	31/12/2018
Task 3	Contribute to the standardization (ECTL)	07/02/2017	01/07/2019
Task 4	Manage and execute SWIM Governance (NATS)	15/05/2018	01/07/2019
Task 5	Legal and financial aspects management (EUMETNET)	01/10/2017	01/07/2019
Task 6	Coordination of common component (AUSTROCONTROL)	07/02/2017	01/07/2019
Task 7	Common Security requirements (ENAV)	07/02/2017	01/07/2019
Task 8	Communication and coordination (DSNA)	07/02/2017	01/07/2019



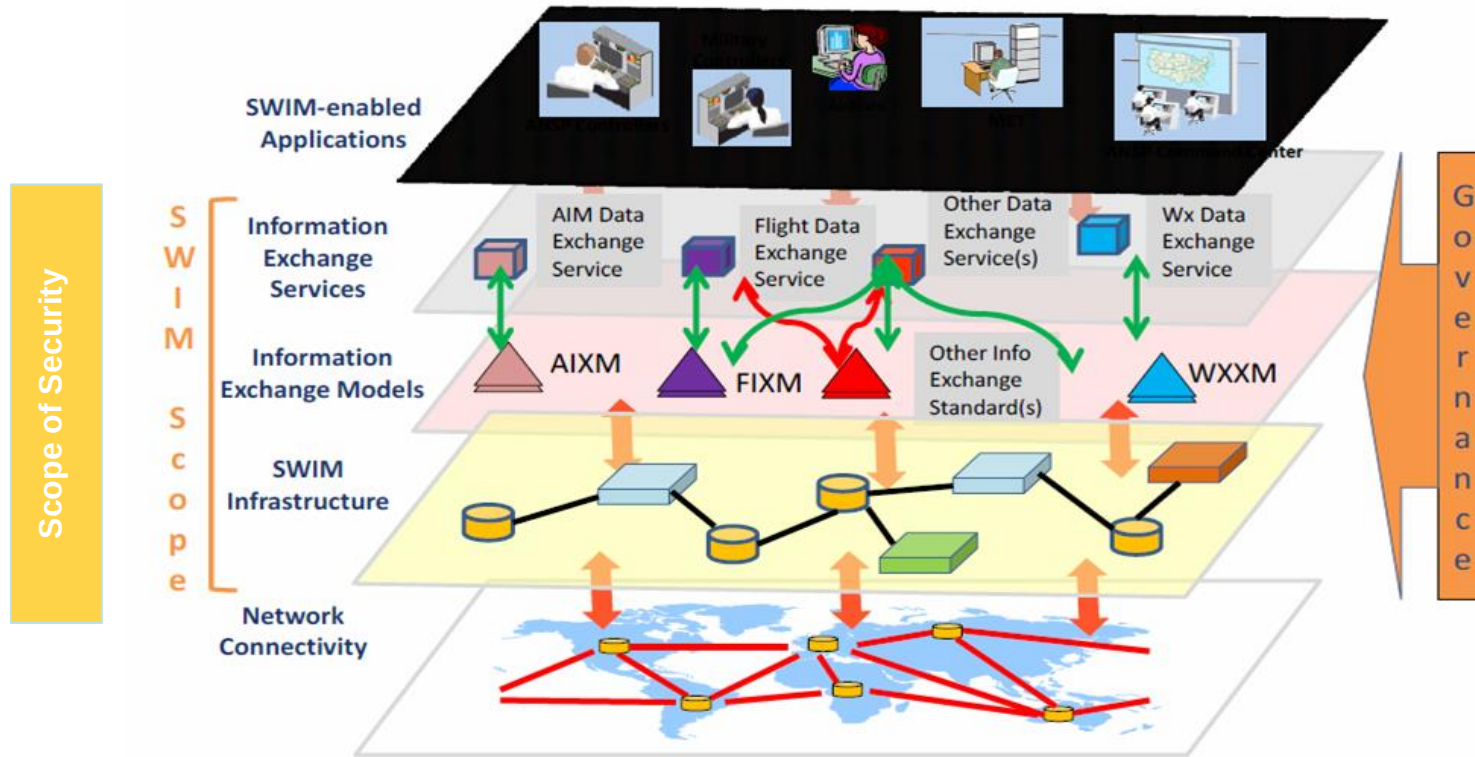
SWIM Governance - Task 7: Description

- Provide specifications for the implementation of an Information Security Management System (ISMS) for SWIM deployment
 - in accordance with European legislation and international standards
 - To be implemented, maintained and continually improved.
- An Information Security Management Plan shall be implemented to define the methodology used, the planned activities and the documents proposed for the security risk assessment
- Cybersecurity is included in the scope of task

**updated according to the requested Action 15.03-11 ref. SWIM Governance kick off meeting MoM (Madrid, Mar 2017), compliant with the agreed option to include relevant “Cybersecurity” domain in the scope*



The context: SWIM Governance layers



SWIM Governance: Task 7 Deliverables

- **D7.1 Security Management Plan** (finalization status)
- D7.2 Risk Analysis
- D7.3 Security Specifications for SWIM



T7 Deliverables: D7.1 Security Management Plan

- Document Structure
 - Confidentiality (Framework)
 - Security Policy
 - Security Management Process
 - Security Risk Analysis, Treatment and Monitoring activity
 - Tools and supporting systems
 - Cyber security testing
 - Cyber security Surveys
 - Collaborative support



References

- ICAO Standards and Recommended Practices
- ICAO guidance material and relevant Docs
- EU SES and NON SES (EC Directive «NIS» 2016/1148)
- ISO/IEC 27000 series and other relevant industrial standards
- Other relevant industrial standards.
- SESAR SecRAM



Confidentiality

Confidentiality framework has been derived from the SESAR2020 Security Framework

- 3 levels of confidentiality are proposed:
 - Low risk material: public documentation
 - Medium risk material: restricted to the project team and distributed according to specific rules (e.g: encrypted docs with password)
 - High risk material: classified information, restricted to single or specific group of people, stored and distributed according to specific rules (e.g: encrypted docs with password)

High Risk

Medium Risk

Low Risk



Security Policy

- Establishes SWIM security as an integral part of SESAR Deployment
- Defines the security organisation within the SWIM Deployment Program and clear lines of responsibility.
- Defines the inter-faces to other programmes and organisations
- Propose the collaborative support of the ATM system to authorities concerned with security incidents

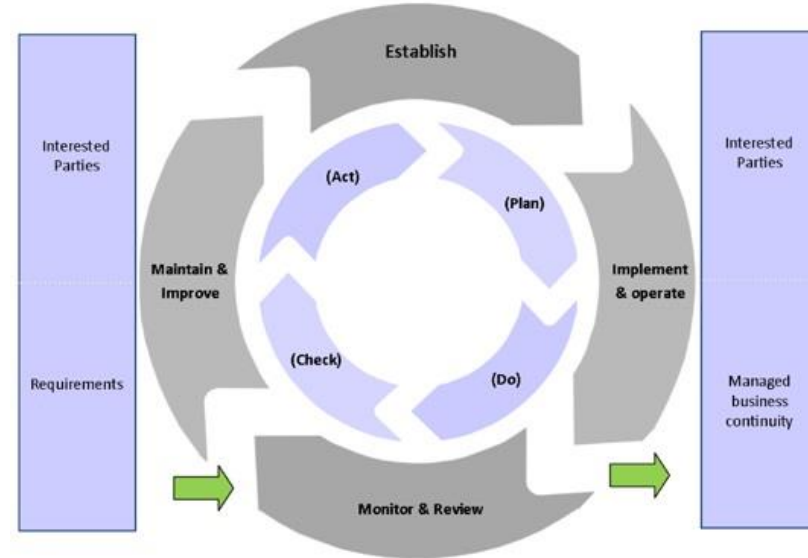
Achieved through:

- The application of Security Management Plan developed by SWIM Governance Task 7
- The application of the Common Security Requirements Material produced by the Task 7



Security Management Process

- Methodology derived from SESAR2020 SecRAM methodology
 - Based on commonly used standard e.g.: ISO27001 family
 - Iterative approach is proposed
 - Primary and Supporting asset analysis and impact
 - Vulnerabilities, Threats exploit and Controls definition
 - Control on Risk of Primary asset is the objective (low risk is the target)
- Monitoring and Review of the process



Cyber security testing & Cyber security Surveys

- It is up to the different stakeholders what testing they want to implement but it is highly recommended to use best-practice on penetration tests, vulnerability assessments and compliance verification.
- The cyber security maturity, status, plan and approach for the different SWIM deployed solution could be measured/investigated by surveys increasing the likelihood of getting relevant requirements



Collaborative Support

Objectives

- Collaboration with agents outside the ATM domain such as law enforcement, military agencies, search and rescue or incident investigation agencies relating to an act of unlawful interference.
- Continuously sharing of information about cyber threats, incidents, vulnerabilities, and other relevant information to relevant authorities through a Security Manager/ Security Staff



Questions?

Alessandro Manzo (Techno Sky / ENAV)
alessandro.manzo@technosky.it

