



PJ.17 Cyber security activities overview and feedback

Laurent VINCENT / Airbus CyberSecurity, laurent.vincent@airbus.com
PJ.17 Cybersecurity focal point

SESAR2020 PJ.17 Open Day, 17th – 18th February 2020
Leonardo Rome, Italy



Founding Members



Project overview



The SWIM-TI provides capabilities enabling decoupled, interoperable , secure and reliable information exchange

PJ.17-01, SWIM Purple Profile (PP), middleware-level support of Air/Ground Advisory Information Sharing to improve ATM operational A/G information exchanges

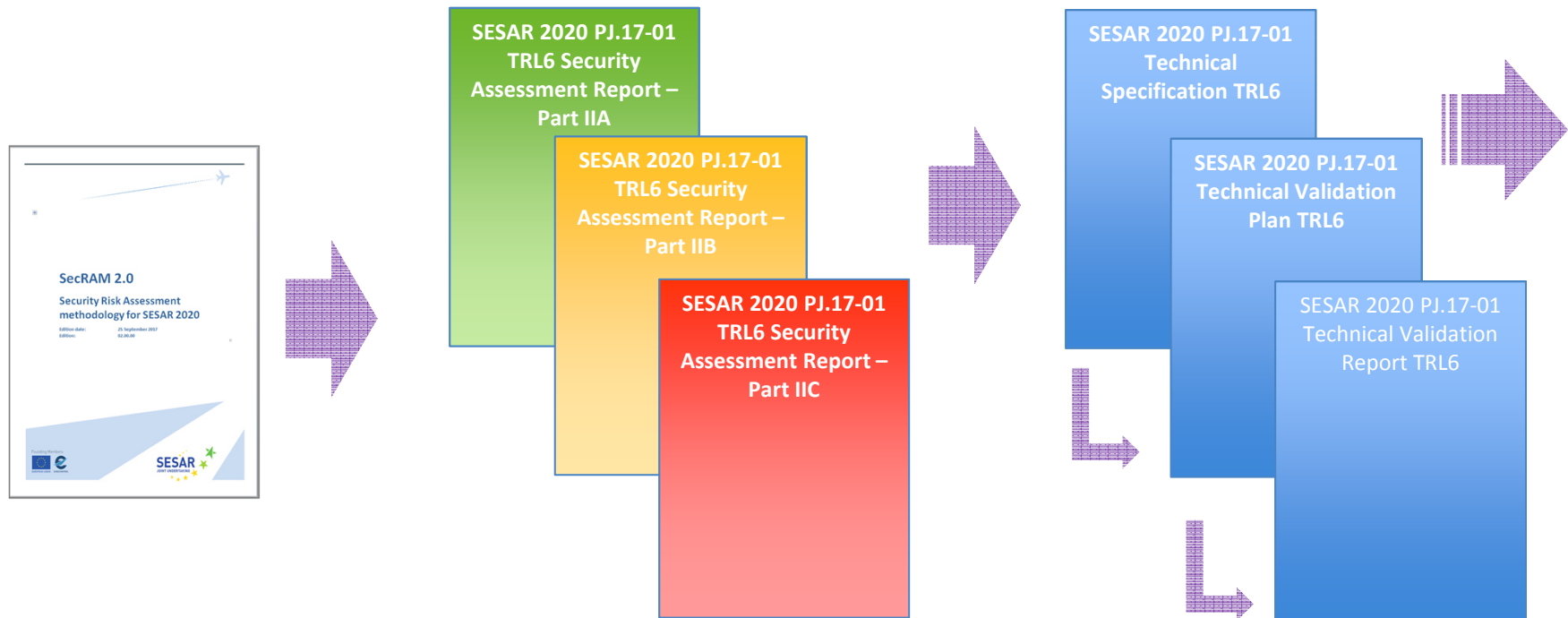
PJ.17-03, SWIM Green Profile (GP), middleware-level support of SWIM-based Ground/Ground (G/G) civil-military data exchanges , full extent of SWIM-based civil-military coordination and cooperation

SecRAM methodology & PJ.17-01 TRL6

Methodology & DELs



- PJ.17-01 identified as prioritized solution in SESAR2020 Cybersecurity context
- PJ.17-01 applied the SecRAM methodology involving in the security risk assessment other solutions (PJ.18-04)



SecRAM methodology & PJ.17-01 TRL6

Identified primary asset



ID	Type	Within scope of security assessment	Outside Scope + Assumptions
SC#1	Inf. exchange		Aircraft control data: Assumption is that this data will not be transported nor affected by SWIM
SC#2	Inf. exchange		ATC Clearance, Instructions or Information: Assumption is that this data will not be transported nor affected by SWIM
SC#3	Inf. exchange	Advisory data	
SC#4	Inf. exchange		Airline business data: Assumption is that this data will not be transported nor affected by SWIM
SC#5	Inf. exchange		Aircraft maintenance data: Assumption is that this data will not be transported nor affected by SWIM
SC#6	Inf. exchange		Passenger and entertainment data: Assumption is that this data will not be transported nor affected by SWIM

SESAR 2020 PJ.17-01 TRL6
Security Assessment Report –
Part IIA



ID	Primary Asset	Type	Description
PA#1	Advisory data	Information	Aeronautical and meteorological advisory data

SecRAM methodology & PJ.17-01 TRL6

Security Assessment Report



- Supporting assets have been identified starting from end2end architecture (application, SWIM-TI and network layers).
- Impact assessment, risk evaluation and treatment have been provided according to the methodology, threats catalogue and identified assets (only SWIM-TI supporting assets).
- Detailed results are confidential and reported in the SAR Part IIB and Part IIC.

SESAR 2020 PJ.17-01
TRL6 Security
Assessment Report –
Part IIB

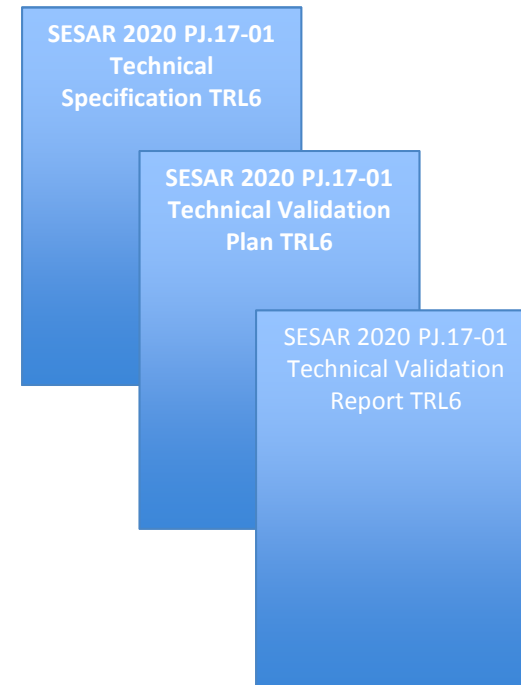
SESAR 2020 PJ.17-01
TRL6 Security
Assessment Report –
Part IIC

SecRAM methodology & PJ.17-01 TRL6

Security Controls



- PJ.17-01 TS TRL6 develops security integration in the different viewpoints (functional, technical, deployment) and traces their multiple relationships (security controls are executed by security functions which are enabled through security technical requirements (“how”))
- Not all the identified security controls were considered subject of technical validation activities. For instance, security controls concerning procedures have been considered out of scope of technical validation activities.
- In the TVALP, Security technical validation objectives are defined starting from ISO/IEC 25010:2011 security sub-characteristics requirements: Confidentiality, Integrity, Non-repudiation, Accountability, Authenticity
- Results from technical validation activities have demonstrated that ,while focusing on “implementation measures” area, the solution contributes positively to the Security KPA



SWIM-TI PP & GP security feedback



Security requirements review

Mainly addresses transport levels security

All security subjects related to deployment and operational aspects out of scope

Additional security controls transferred due to the limited scope of the solution

Risk analysis assessment

Effective use of SecRAM as an homogeneous method across solutions

Feedbacks on SecRAM methodology usage and improvement

Successful reduction of risks identified at design and validation level

Next steps recommendations

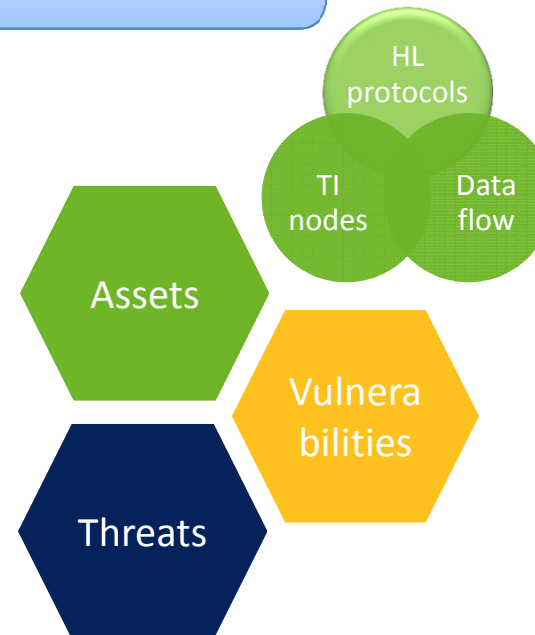
Ready to use and suitable SecRAM in Wave 2

Dynamic and extended
catalog approach

Include vulnerability study at
early stage

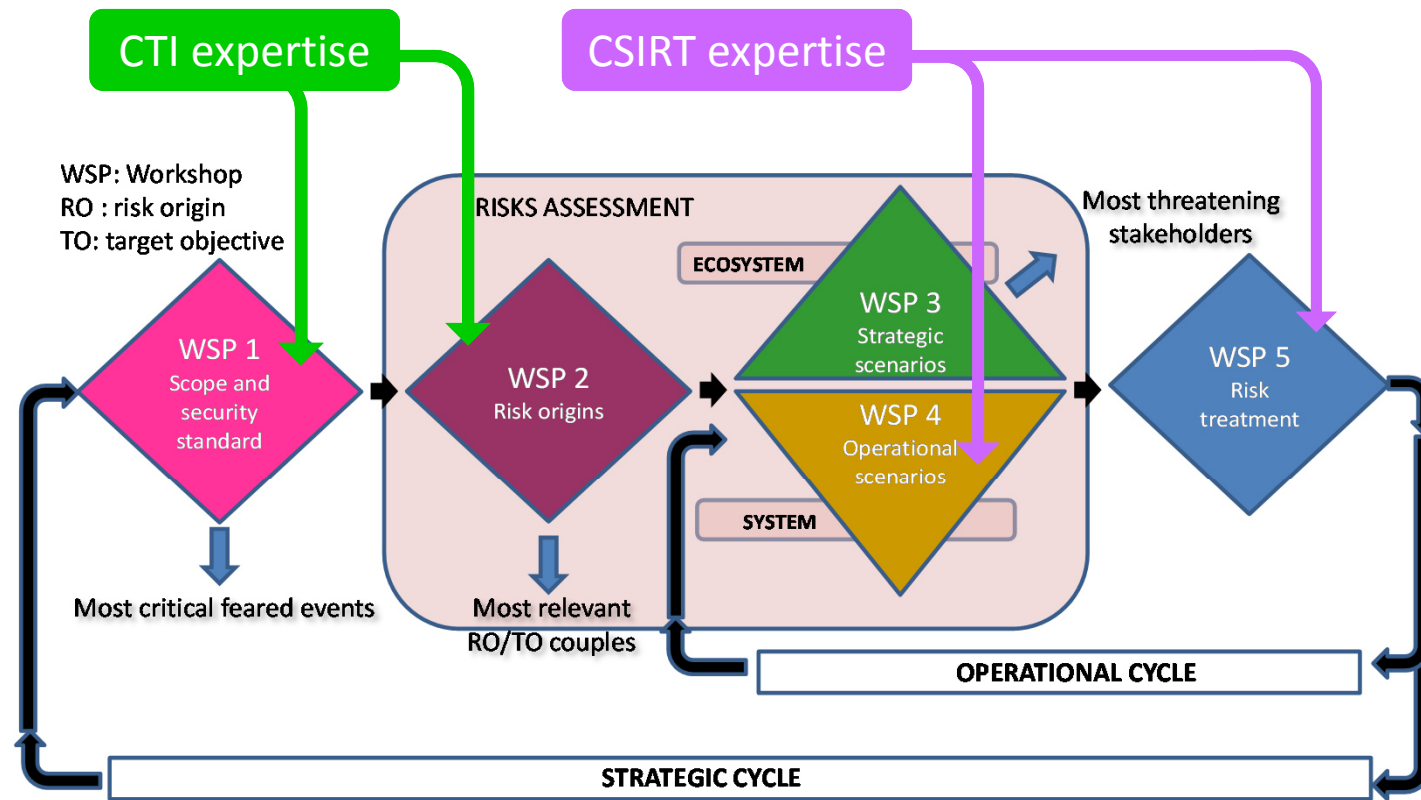
Add system life-cycle
requirements

Extend to military usages



SecRAM more than just a delivery item
It must provide training and support program on risk
assessment methodology

AI DS Cyber Advanced EBIOS Risk Manager



EBIOS RM risk analysis method from ANSSI
Cyber attack scenario based

Solution objectives adaptable toolbox
AI DS Cyber enhancement with CTI and
CSIRT expertise contribution

Q&A





PJ.17 Cyber security activities overview and feedback

Thank you very much for your attention!



This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No [number]



Founding Members



The opinions expressed herein reflect the author's view only.

Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.