SecRAM 2.0

Security Risk Assessment methodology for SESAR 2020

Edition date: 25 September 2017
Edition: 02.00.00

Founding Members

EUROPEAN UNION EUROCONTROL

SESAR JOINT UNDERTAKING

Authoring & Approval

Author(s) of the document

Name	Organisation	Date
Miriam le Fevre	COOPANS	20/09/2017
Birgit Gölz	DFS	20/09/2017
Ruben Flohr	SESARJU	20/09/2017
Tim STELKENS-KOBSCH	DLR	20/09/2017
Theo VERHOOGT	NLR	20/09/2017

Reviewed by

Name	Organisation	Date
Eric BILLARD	EUROCONTROL	26/09/2017
Roman NOSSAL	AUSTROCONTROL	26/09/2017
Maria Doris DI MARCO	ENAV	26/09/2017
Stephen WILLIAMS	NATS	26/09/2017
Frederique ROUSSEAU	ATOS	26/09/2017
Antonio STRANO	LEONARDO	26/09/2017
Norman STEWART	AIRTEL	26/09/2017
Peter DAVIS	NCSC	26/09/2017
Philippe MORIO	DSNA	26/09/2017
Sujan PERERA	NATS	26/09/2017
Michel PROCOUDINE	THALES	26/09/2017
Mikael MÅNSTRÖM	LFV	26/09/2017

Approved by

Name	Position/Title	Date
PC #04	Programme Committee #04	13/10/2017
CCB #20	Programme Change Control Board	03/11/2017

Document History

Edition	Date	Status	Author	Justification
00.00.01	07/04/2017	Draft	Ruben/Miriam	Initial structure
00.00.02	02/08/2017	Draft	Birgit/Miriam	Process input taskforce
00.01.00	19/09/2017	For review	Birgit/Ruben	Text made more concise
02.00.00	03/11/2017	Final	Birgit/Ruben	Baselined as programme guidance

This version of the SecRAM methology is an update to the final version under SESAR 1. Changes have been made to enable a differentiated approach depending on maturity level and the solution evaluation in the initial security assessment.

The following people have been responsible for creation and reviewing of the SecRAM 1.0 version from SESAR 1:

John HIRD (EUROCONTROL), Chris MACHIN (AZTECH), Martin Hawley, Erwan HAMON (AIRBUS), Birgit GÖLZ (DFS), Maria Doris Di Marco (ENAV), Roman MADARASZ (FREQUENTIS), Jorge ALEMANY (INDRA), Patrizia MONTEFUSCO (FINMECCANICA), Philippe JASSELIN (THALES), Jérôme Chaigneau (AIRBUS), Edouard Painchault (THALES), Gilles Descargues (THALES AVIONICS).

Copyright Statement

Abstract

This document presents the SESAR2020 ATM Security Reference Material, explaining methods, tools and techniques to deliver Evidence necessary for an ATM Cyber Security Risk Assessment.

Based on the methods and techniques of the SecRAM material from SESAR 1, this document adds the notion of security-prioritized and security non-prioritized solutions applied in SESAR2020 and defines which SecRAM steps are mandatory for the different solution maturity levels.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose

1.1.1 Purpose of the document

This document provides the methodology and practical guidance for solution projects when building their Cyber Security Risk Assessment. It presents the requirements for demonstrating that a SESAR Solution has adequately addressed ATM security in the research and development phase of SESAR, thus ensuring that the outcome is a securable solution.

1.1.2 Changes since the previous version

This version of the document is an update to the final version under SESAR 1. Changes include a differentiated approach depending on maturity level and the security prioritisation.

1.1.3 Glossary of terms

Term	Definition
Asset	Elements in the system that have value for the achievement of business objectives or element that support the existence of the business objectives.
Attacker	A person, entity or organisation causing a threat with malicious intent.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Cyber Security Control	Cyber security controls are defined to protect supporting assets. They are a collection of measures to ensure that the Cyber Security Objectives are met. They are a means of managing risk, including procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.
Cyber Security Risk Level	For each threat scenario, the combination of its likelihood with its security impact gives the associated risk level.
Cyber Security Objective	A measurable statement of intent relating to the protection of a primary asset.
Cyber Security Requirement	A tangible condition that needs to be in place in order to meet the Cyber Security Objectives.

Term	Definition
Impact	The extent to which a loss of confidentiality, availability or integrity of an asset affects the achievement of business objectives. An evaluated consequence of a particular event.[1]
Integrity	The property of safeguarding the accuracy and completeness of assets. Data integrity is the opposite of data corruption, which is a form of data loss. Data integrity aims to prevent malicious changes to information.
Likelihood	The probability that an identified impact to a Primary Asset will occur.
Primary Asset	Intangible function, service, process or information that are part of the ATM system within the scope of the project and has value to the system. They are information and services that are valuable in the sense that a successful attack impairing them will mean harm to the ATM system in terms of personnel, capacity, performance, etc.
Residual security risk [1]	The security risk remaining after security risk treatment.
Resilience [1]	Ability of an organisation to resist being affected by an event.
Reviewed Impact	This is an adjustment of the inherited impact due to existing or planned controls, which will be in place to reduce the impact. These controls will relate to reducing the impact rather than reducing the likelihood of attack.
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby have an impact on the ATM service.
Security incident [1]	Intentional event that might be, or could lead to, an operational interruption, disruption, loss, emergency or crisis.
Supporting Asset	A ***Supporting Asset is a*** tangible element that supports the existence of the primary assets. Entities involved in storing, processing and/or transmitting primary information assets are classified as supporting assets. Examples are hardware, software and people.
System	Any element to support the ATM function including hardware, software, people, procedures and processes
Threat	A potential cause of a cyber security incident.
Threat Scenario	A threat scenario is the chain of events or occurrences that take place starting with one or more threats and ending with the consequences of an incident.

[1] ISO 22399:2007

Term	Definition
Vulnerability	Vulnerability is a characteristic of supporting assets. The vulnerability of an asset is determined by a potential weakness in operational processes and procedures, physical security or technical gap, which can be exploited by a threat source to trigger a threat scenario. Vulnerabilities of supporting assets are the paths through which threats can reach primary assets and impair them.

1.1.4 Acronyms and Terminology

This table captures general Acronyms and Terminology for ATM Security.

Term	Definition
ATM	Air Traffic Management
CIA	Confidentiality, Integrity, Availability
E-OCVM	European Operational Concept Validation Methodology
OSED	Operational Service and Environment Description
PA#	Primary Asset identifier
SA#	Supporting Asset identifier
SecRAM	Security Risk Assessment Methodology
TRL	Technology Readiness Levels

2 Theory of security

2.1 What is cyber security?

2.1.1 Physical security versus cyber security

The new EU Network and Information Systems (NIS) Directive states that a reportable incident is:

- Any event that has an actual adverse effect on the security of network or information systems used in the provision of essential services;
- where the security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems; and
- One that has a significant impact on the continuity of essential services they provide.

It is important to note that the NIS incident reporting requirements are not limited to "cybersecurity" incidents: any incident affecting the security of the network and information systems used for provision of the essential services may be reportable. This will include physical events where there is an impact on the security of a relevant network and information system

From this it can be seen that in the SESAR context cyber security cannot confine itself to attacks which are delivered through Information Technology (IT) and Operational Technology (OT) systems and must include all causes of impact. A comprehensive risk management system will enable this to happen.

2.1.2 Safety management versus cyber security management

A common observation in safety critical contexts is that there can be difficulties in integrating a system's security and safety requirements. Where this occurs, this is likely to be an indication that security has only been analysed from a component (supporting assets) perspective.

If one looks at a system from the Functional Purpose level of abstraction (primary assets), the distinction between safety and security becomes less relevant, as the impact analyses start overlapping[2]. As noted above, at this level of abstraction, risks are described in terms of high-level losses, such as the system causing death or injury. Whilst such a loss might appear to be solely a safety concern, a cyber attack could lead to the same impact (people's death and injury) that safety practitioners are concerned with.

This is not to say that safety and security are one and the same thing. They are clearly different disciplines with different professional expectations. The point here is that viewing a system's risks

[2] At least partially, related to people's death and injury. For other areas like economic and branding impact security impact analysis is broader in scope.

from its most abstract perspective can give safety and security practioners a shared language with which to discuss their work, and to trade requirements according to how they support common objectives, such as reducing the likelihood of death or injury.

There are practical differences between the established approaches to security and safety that present difficulties in integrating or interfacing the two domains. Notwithstanding this, it is clear that the safety risk analysis and the security risk analysis must at least not conflict and efficiency dictates they should be done with all necessary exchange of information. This wil include providing the necessary traceability between security risk and safety-significant outcomes, as well as the controls and governance at the interfaces between the two domains to ensure consistent presentation to the accountable stakeholders of the overall risk to the ATC system.

2.1.3 Cyber resilience

The idea of resilience, in its most basic form, is an evaluation of what happens before, during and after a digitally networked system encounters a threat. Resilience is not event-specific: it accrues over the long term and should be included in overall business or organizational strategy. From a policy-making perspective, one challenge regarding cyber-resilience is the fact that no global definition exists. Therefore only limited agreement exists on how to achieve it.

This section consequently introduces the understanding of resilience as it is expected to be used throughout the action paper and expected to be understood when applied to the solutions under consideration.

In order to develop the methods and advice as well for the procedures as operations the essential pre-requisite is an agreement about definitions. There are manifold definitions about resilience when looking to ATM, IT or beyond. The different understandings of resilience describe a combination of different properties. Some target on foresight, robustness, resourcefulness, redundancy, rapid recovery and adaptability. Others take prevention, preparedness, respond and recovery into consideration. Even in ISO and NIST the definition of resilience is still evolving.

In order to set the framework conditions for this action paper the following definition of resilience in the context of cybersecurity for S2020 is used:

*Resilience is the ability to **prevent** disruptions, to **prepare** for and adapt to changing conditions and to **respond** and **recover** rapidly from disruptions to ensure the continuity of **services** at an acceptable performance level.*

The aim of this definition is not at last to achieve the understanding that caring for resilience is more affiliated to the management of risks than to the elimination of them.

Being resilient implies minimising reductions in performance (acceptable drop of performance) in the face of a succesful attack. This means the solution under development needs to be able to work properly also in several levels of degraded mode, while healing measures and repair works can be undertaken. This degraded mode needs to be kept until the effects of an attack have been assessed and accounted for. Having stated this, it is furthermore essential to provide methods and means to allow the solution to recover as quick as possible from such degraded modes (minimum recovery time).

2.1.4 Resilience by design: Prevent, prepare, respond and recover

Prevent, prepare

The whole set of measures required for sufficient resilience against cyber attacks is a combination of different actions and proper behaviour. The flow of cyber resilience actions already starts when the services, tools or systems under concern are in the development phase. This often is related to the phrase “security by design”. For the issues discussed herein it shall be rephrased as “resilience by design”.

For networked technologies, vulnerability in one node can affect the security and resilience of the entire network. Since cyber resilience is a matter of risk management, there isn’t a single point at which it begins or ends. Instead, it comes from building a strategy and working to ensure that the risk-management mechanisms that work for more traditional threats are also brought to bear on new cyber threats.

Emphasis needs to be put on the architectural layout of solutions. Vulnerabilities which may be exploited by adversaries often have their source in architectural deficiencies. This is true not only for comprehensive solutions but especially for the interfacing to other systems, system elements or tools. When taking this into account a first step of **prevention** is achieved. Controls may have to be put in place to address potential risks emanating from other parts of the “system of systems”.

Respond, recover

Another pillar of resilience is to **prepare** for possible attacks. This can be achieved by procedures and training of staff. Being prepared for any cyber attack begins with thinking about daily activities and the way work is organised and conducted. This includes also the knowledge (and hence training) about the fastest and most secure ways of de-coupling software tools from the system or network and safely/securely shutting down infected systems.

When being under attack from outside (or even inside) the **response** to the attack is also important. The first response focusses on identifying the problem, containing it, eradicating it. Responsive measures may also include the restriction of services or the unwinding of trained sequences[3]. The focus shall be kept on the secure delivery of services and data whilst being aware of the attack in progress.

The response phase needs to be continued until the cause and even the cascading effects of the attack have been eliminated, accounted for or phased out. When at any point in time this can surely be confirmed the phase of **recovery** may be initiated. This phase again needs to be as short as possible in order to have all services, tools and systems in full operation after a cyber attack

[3] The response and recovery phases are performed on operational systems during Incident Management, which is not directly in the scope of the R&D activity. Nevertheless, some of the standard controls which will be recommended will contribute to the effectiveness of the incident management process. (e.g. change management, backups, etc).

2.1.5 Security controls

In order to achieve cyber-resilience and the required level of security, security controls[4] have their effect either pre-event or post event (see figure 1):

- Pre-event controls can reduce the likelihood an incident OR the impact if the attack is successful;
- Post-event controls reduce the impact by, for example, limiting the duration, geographical scope or operational services impacted.

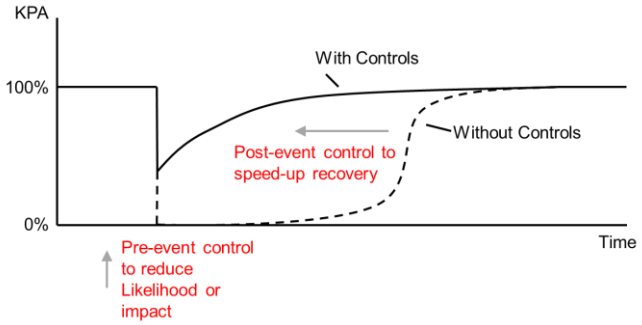


Figure 1 Pre-event and post-event controls

2.1.6 Defense in depth vs strength of control

When setting up the strategy of protection two different approaches may be chosen: defence in depth or strength of control.

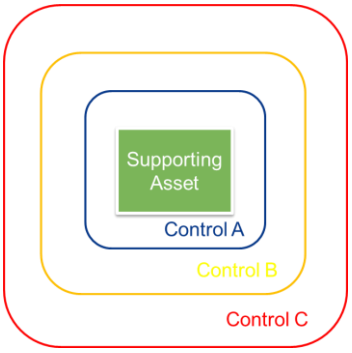


Figure 2: Defence in Depth

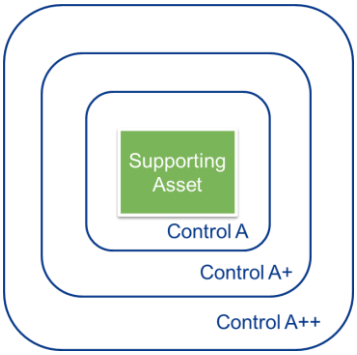


Figure 3: Strength of Control

Defence in depth refers to a multi-layered set of unrelated controls acting together to provide protection to a supporting asset (and hence the related primary asset). The multi-layered approach

[4] In SESAR 1, the notion of the Minimum Set of Security Controls (MSSC) had been developed. These controls, most of them being generic and organisational of nature, have been integrated as pre-requisite for any organisation involved in industrialisation or deployment and for any solution pack provided by SESAR. This is considered sufficient for security non-prioritized solutions. For security-prioritized solutions a new catalogue of solution specific controls has been created within SESAR 2020, based on the ISO 27002 – 2013 catalogue.

to controls means that if one control is compromised then another control should act as the next layer of defence.

The concept of the **strength of a control** is to improve the performance of one 'type' of control, for example access control, personnel security or encryption. This means an attacker needs more expertise, money, tools and skill to break through the control as its protection has been strengthened.

The objective of a security control implementation is that the combination of these groups of security controls achieves a level of protection, which is sufficient to meet the cyber resilience objectives for all the defined risks, while taking into account cost, control effictiveness, risk mitigation impact, architectural consistency, minimise impact on system performance, minimise impact on safety.

2.2 Technology Readiness Levels

SESAR 2020 Programme covers Technology Readiness Levels (TRL) 2-7[5].

Where a topic description refers to a TRL, the following definitions apply, unless otherwise specified:

- TRL 1 – basic principles observed
- TRL 2 – technology concept formulated
- TRL 3 – experimental proof of concept
- TRL 4 – technology validated in lab
- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
- TRL 7 – system prototype demonstration in operational environment
- TRL 8 – system complete and qualified
- TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Figure 4TRL-levels ref Commission Decision C(2014)4995 Part 19

As the SESAR Programme covers not only technology, but also concepts, the European Operational Concept Validation Methodology (E-OCVM) is used in the projects.

[5] Reference SESAR 2020 Multi-Annual Work Programme

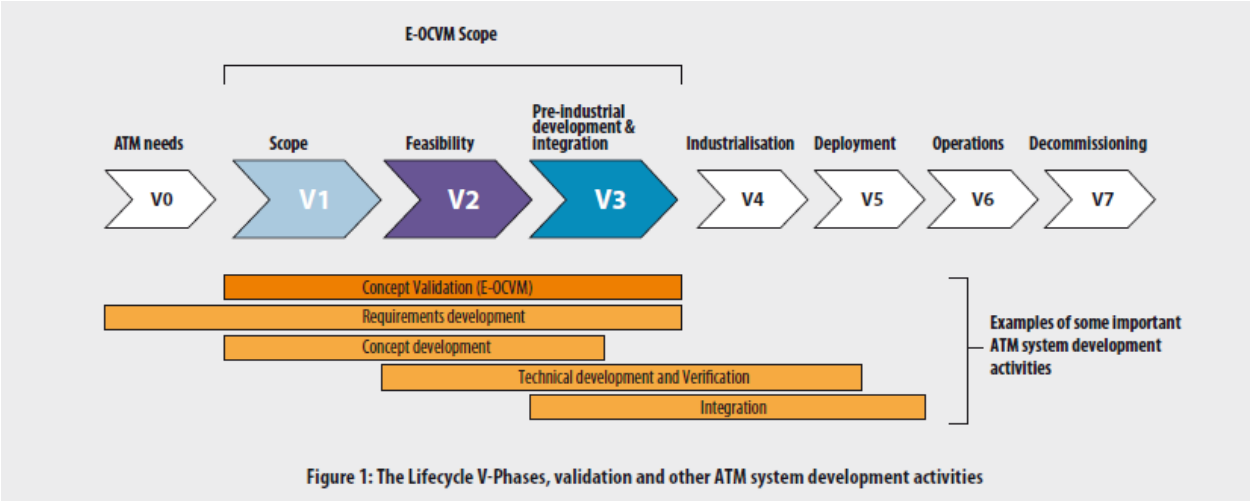


Figure 1: The Lifecycle V-Phases, validation and other ATM system development activities

Figure 5 E-OCVM lifecycle

2.3 Securable and cyber-resilient solutions

In SESAR 2020 the notion of security-prioritisation has been introduced. The SESARJU's scope is limited to the R&D phases up to E-OCVM V3, or TRL6. The industrialisation and deployment phases will only be done after the SESARJU has completed its R&D. Many aspects of security will only be implemented during industrialisation or even deployment. Examples include incident management, systems hardening or ensuring security clearances for operational and technical personell. Although many aspects will only be implemented later, the majority of the security controls corresponding to industrialisation and deployment will have been anticipated during the security risk assessment in R&D and captured as security requirements of the solution pack.

The SESAR programme distinguishses itself from regular systems development through its "system of systems" approach, building an environment of many systems from many stakeholders being interconnected through dependencies. This drives the need for a deeper understanding of stability and resilience of such a "system of systems", also from a cyber security perspective.

Driven by the need for effective resource usage, the SESAR2020 security strategy postpones effort on security where risk wise acceptable, as long as it is ensured that the solutions delivered can be secured in the post-R&D phases. Key is to deliver ***securable*** and ***cyber-resilient*** solutions.

2.4 Cyber Security in SESAR 2020

As SESAR 2020 is dealing with R&D and therefore not fully mature solutions ready for deployment, risk assessment has to be performed step-wise. The steps are identified in this methodology based on "just-in-time" principle.

With the notion of securable and cyber-resilient solutions in mind, priority is given to security activities for solutions that improve the understanding of cyber-resilience, solution that come with a substantial risk of delivering an un-securable solution if security were not properly addressed during R&D, and those solutions that address technologically complex architectures or use new technologies.

This line of thought has been translated to the following criteria that result in a solution to be security-prioritized.

1. Cyber-attack could lead to an accident or serious safety incident
2. Cyber-attack could lead to capacity reduction to less than 25% of normal operations
3. Cyber-attack could have high negative economic impact on multiple stakeholders throughout Europe
4. Cyber-attack could have a negative impact on military systems (WOC/flight deck)
5. Cyber attack could lead to the loss of a high number of functionalities essential for the provison of ANS. This relates to the level of integration.

The consideration of “technologically complex architectures” or use of “new technologies” is obvious, and the assessment of the need to prioritize requires expert judgement that looks at the potential influence of security considerations on architectural options, use of new technologies, use of existing non-encrypted data, use of wireless connections, use of other unsecured interfaces. For each of these aspects possibly already availbale security material will also be taken into account.

For each solution, an prioritisation assessment is performed based on the above criteria, determining whether the solution shall be handled as “non-prioritized” or “prioritized”. The security material to be produced depends both on the prioritisation and the target maturity level, as defined in the next chapter.

2.5 The security risk assessment methodology

Security risk assessment is a process to identify and mitigate the consequences of an attack. It defines a set of security requirements to ensure that if an attack takes place the consequences have been estimated and can be managed and may contribute to the recovery of normal operations in a reasonable time.

Risk Management encompasses Risk Assessment and Risk Treatment. This is an important distinction as risk assessment and treatment may be led by different working groups.

Risk assessment is an iterative process, that needs to be iterated by adding controls untill the residual risk meet the cyber security objectives.

The steps of security risk assessment are:

- Define the scope of the risk assessment (description of involved roles, equipment, systems...) and the identification of dependencies on other systems and infrastructure. To perform this step, specialist operational or design knowledge of the system is required.

- Identify assets and valuate possible impacts on assets: assets form the targets of security attacks, and the identification of possible impacts is concerned with evaluating the harm resulting from each asset being compromised by an attack.

- Identify vulnerabilities, threats and likely threat combinations: it comprises the identification of possible (or credible) threat sources and related threat scenarios. Each threat is associated to vulnerabilities of the system that can be exploited by an attacker.

This group of activities aims at providing an insight into all routes through the system (threat scenarios) that a threat may use to access an asset.

- Identify a set of security controls that act upon the supporting assets, that will reduce the impact on Primary Assets, and evaluate the impact on Primary Assets after implementation of the security controls.

  Note: A first iteration of the risk evaluation may be conducted with controls limited to those already in operations (see environmental assumptions, section 5.2) and generic organisational controls (e.g. from MSSC, see footnote on page 11) to ensure focus only on the identification of controls that mitigate risks that do not meet the programme generic security objective.

- Determine the likelihood of the impact on Primary Assets to occur
- Assess the security risk
- Determine whether the security risk is within the acceptable level set by the Cyber Security Objectives – if not, it is necessary to go back in the process to identify how the situation can be improved.

The need for prioritisation should be reevaluated at each maturity gate.

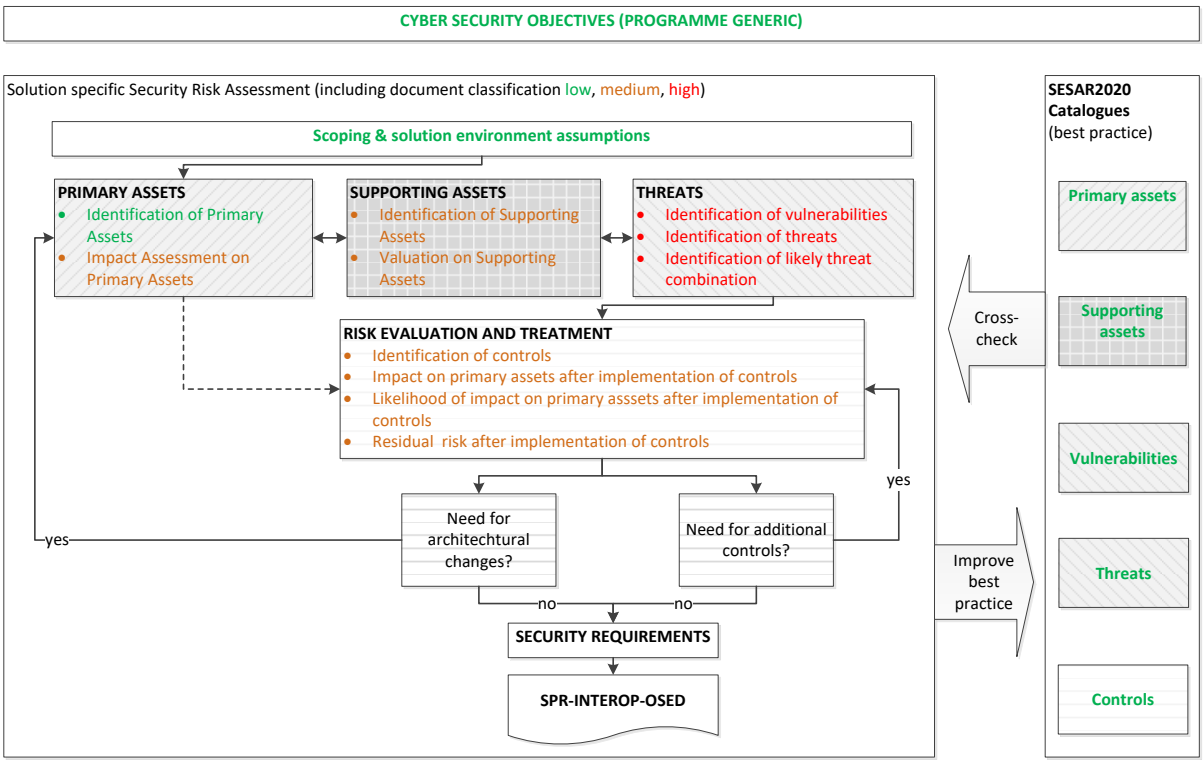


Figure 6 The SecRAM methodology

3 Checklists

3.1 Checklist prioritized solutions

The tables below indicate for prioritized solutions the need to address - or the possibility to skip - a SecRAM step at any of the solution maturity levels. Each step is described in more detail in chapter 5.

Cyber Security Objectives (PROGRAMME GENERIC)

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Cyber Security Objectives	**GIVEN**	GIVEN	GIVEN	GIVEN

Scoping & solution environment assumptions

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Scoping & solution environment assumptions	**INITIALISE**	Update	Update	Update

Primary Asset identification and impact assessment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Primary Assets	**INITIALISE**	Update	Update	Update
Impact Assessment on Primary Assets	**INITIALISE**	Update	Update	Update

Supporting Asset identification and valuation

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Supporting Assets		**INITIALISE**	Update	Update
Valuation on Supporting Assets		**INITIALISE**	Update	Update

Threats

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Vulnerabilities		**INITIALISE**	Update	Update
Identification of Threats		**INITIALISE**	Update	Update
Identification of Likely Threat combinations		**INITIALISE**	Update	Update

Risk evaluation & treatment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Controls		**INITIALISE**	Update	Update
Impact on Primary Assets after implementation of Controls		**INITIALISE**	Update	Update
Likelihood of impact on Primary Assets after implementation of Controls		**INITIALISE**	Update	Update
Residual risk after implementation of controls		**INITIALISE**	Update	Update

Security requirements

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Capturing controls as security requirements		**INITIALISE**	Update	Update

3.2 Checklist non-prioritized solutions

The tables below indicate for non-prioritized solutions the need to address - or the possibility to skip - a SecRAM step at any of the solution maturity levels. Each step is described in more detail in chapter 5.

Cyber Security Objectives (PROGRAMME GENERIC)

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Cyber Security Objectives	**GIVEN**	GIVEN	GIVEN	GIVEN

Scoping & solution environment assumptions

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Scoping & solution environment assumptions	**INITIALISE**	Update	Update	Update

Primary Asset identification and impact assessment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Primary Assets	**INITIALISE**	Update	Update	Update
Impact assessment on Primary Assets	**INITIALISE**	Update	Update	Update

Supporting Asset identification and valuation

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Supporting Assets		**INITIALISE**	Update	Update
Valuation on Supporting Assets		**INITIALISE**	Update	Update

Threats

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Vulnerabilities		Optional	**INITIALISE**	Update
Identification of Threats		Optional	**INITIALISE**	Update
Identification of Likely Threat combinations		Optional	Optional	Optional

Risk evaluation & treatment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Controls		Optional	Optional	Optional
Impact on Primary Assets after implementation of Controls		Optional	Optional	Optional
Likelihood of impact on Primary Assets after implementation of Controls		Optional	Optional	Optional
Residual risk after implementation of controls		Optional	Optional	Optional

Security requirements

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Capturing controls as security requirements		Optional	Optional	Optional

4 Practical guidance

4.1 Cyber Security Objectives (PROGRAMME GENERIC)

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized	**GIVEN**	GIVEN	GIVEN	GIVEN
Prioritized	**GIVEN**	GIVEN	GIVEN	GIVEN

Description	A solution's cyber-security objective defines the level of residual risk that is acceptable for each of its primary (operational) assets. The residual risk is assessed after the application of security controls to reduce impact of a successful attack (contingency measures) and to reduce the likelihood of a successful attack (security controls). **Impact** **Likelihood** / **1** / **2** / **3** / **4** / **5** **5** / Low / High / High / High / High **4** / Low / Medium / High / High / High **3** / Low / Low / Medium / High / High **2** / Low / Low / Low / Medium / High **1** / Low / Low / Low / Medium / Medium **The cyber security objective is defined at a programme level. Solution specific residual risk at medium level needs to be justified in the security annex. Residual risk as high level is not acceptable.**
Examples	Not applicable
Tool support	Not applicable
Catalogue / Table	Not applicable
How to document	Not applicable, these objectives re-appear in section 5.7.4
Security classification	Low risk, general distribution within aviation domain okay

4.2 Scoping & solution environment security assumptions

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized	**INITIALISE**	Update	Update	Update
Prioritized	**INITIALISE**	Update	Update	Update

<table>
<tr><td>Description</td><td>Define the scope of the risk assessment (description of involved persons, equipment, systems...) and the identification of dependencies on other systems and infrastructure.

A solution always operates in an environment that already exists, and to which it connects. When performing a security risk assessment, the boundaries of the security risk assessment have to be identified. Assets within the boundaries are identified and assessed, whereas for assets outside the boundaries assumptions on the security of the environment to which the solution interfaces have to be made explicit. If the security of the environment cannot be assumped to be sufficiently secured, leading to an medium or high risk, controls need to be identified to protect the solution at its boundaries.

To perform this step, specialist operational or design knowledge of the system is required.

Note: In case of partial overlap or tight integration, a security risk assessment may be conducted as a joint effort between two or more solution projects. Building on already available security risk assessment material for integration, adjustment and improvement is also considered good practice.</td></tr>
<tr><td>Examples</td><td>Solution 17-01 investigates the SWIM TI Purple Profile for A-G Advisory Info Sharing. Its core business is the message routing between airborne and ground SWIM nodes.

<table>
<tr><th>ID</th><th>Type</th><th>Within scope of security risk assessment</th><th>Outside Scope + Assumptions</th></tr>
<tr><td>SC#01</td><td>Information exchange</td><td>Aircraft advisory (e.g. AIS/MET) data.</td><td>Aircraft control data: Assumption is that this data will not be transported nor affected by SWIM.</td></tr>
<tr><td>SC#02</td><td>Information exchange</td><td></td><td>ATC Clearance, Instructions or Information: Assumption is that it will not be transported by SWIM, but in Step 2 both ATC and SWIM will use the same IP network.</td></tr>
<tr><td>SC#03</td><td>Information exchange</td><td></td><td>Passenger and entertainment data: Assumption is that that this data wil be transported on a</td></tr>
</table>
</td></tr>
</table>

	different IP network.
Tool support	No tool support until further notice
Catalogue	Not applicable
How to document	**ATM solution projects** • See Low Risk material section 1.1 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIA - Security Assessment Report" **Enabling solution projects** • See Low Risk material section 1.1 "SESAR 2020 TS-ISR - Template - Part IIA - Security Assessment Report"
Security classification	Low risk, general distribution within aviation domain okay

4.3 Primary Assets

4.3.1 Identification of Primary Assets

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized	INITIALISE	Update	Update	Update
Prioritized	INITIALISE	Update	Update	Update

Description	Primary assets are the intangible activities, information and services that are of value and need to be protected. A successful attack would ultimately impair the primary assets and have an impact on the ATM system. It is recommended to apply SecRAM to the service level of the project as here it is easy to distinguish between information flows/data flows, data elements and interfaces to other services. These are called primary assets.

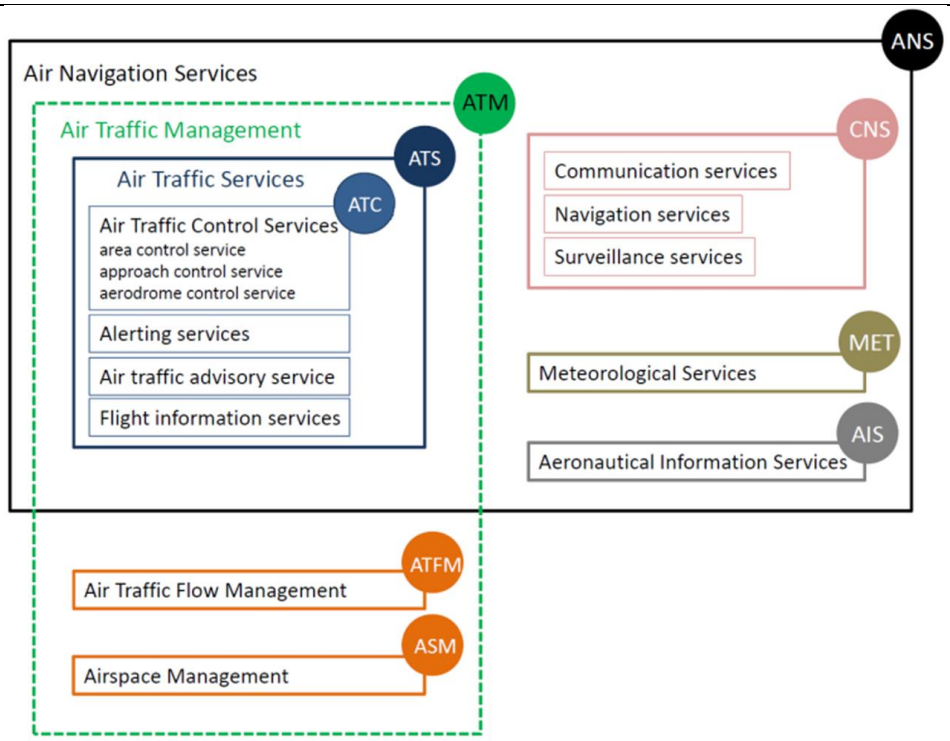


Figure 7: Components of ATM

Services which may be considered as primary assets may include:

- Services whose loss or degradation make it impossible to carry out the mission of the project.
- Services that contain classified processes or processes involving proprietary technology.
- Services that, if modified, can greatly affect the accomplishment of the project's mission.
- Services that are necessary for the project to comply with contractual, legal or regulatory Requirements.

Information which may be considered as primary assets include:

- Vital information for the exercise of the project's mission or business.
- Personal information, as can be defined specifically in the sense of the national laws regarding privacy
- Strategic information required for achieving objectives determined by the strategic orientations
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

To determine if an asset can be considered as primary, the following question can be used:

> *Does compromising the confidentiality, integrity or availability of the asset have a negative impact on the ATM system in some of the following SESAR security impact areas: personnel, capacity,*

<table>
<tr><td></td><td>performance, economic, branding, regulatory and environment?

A positive answer to this question means that the asset must be included in the list of primary assets.

Another way of identifying primary assets is to try to establish a link between assets and goals of potential attackers: those assets that might be targeted for attacks and which may have a security impact if they are compromised (i.e. not working as originally intended).</td></tr>
<tr><td>Examples</td><td>
<table>
<tr><th>ID</th><th>Primary Asset</th><th>Type</th><th>Description</th></tr>
<tr><td>PA#1</td><td>Collision Avoidance</td><td>Service</td><td>Safety net in case separation has been breached.</td></tr>
<tr><td>PA#2</td><td>Area Control</td><td>Service</td><td>Air Traffic Control service for the en-route traffic</td></tr>
<tr><td>PA#3</td><td>Meteorology Information</td><td>Information</td><td>This information includes airport weather forecast and nowcast, as well as high weather forecast.</td></tr>
<tr><td>PA#4</td><td>Surveillance Information</td><td>Information</td><td>Aircraft position information acquired through e.g. PSR, SSR, ADS-B or MLT.</td></tr>
</table>
</td></tr>
<tr><td>Tool support</td><td>No tool support until further notice</td></tr>
<tr><td>Catalogue</td><td>See “SecRAM catalogue, tab “Primary Assets”. The use of this catalogue is not restrictive, but should be considered as guidance material. To improve best practice in SESAR 2020, after solution level brainstorming new elements for re-use by other projects can be proposed to PJ19 for inclusion.</td></tr>
<tr><td>How to document</td><td>ATM solution projects

• See Low Risk material section 2.1 “SESAR 2020 SPR INTEROP OSED - Template - Part IIIA - Security Assessment Report”

Enabling solution projects

• See Low Risk material section 2.1 “SESAR 2020 TS-IRS - Template - Part IIA - Security Assessment Report”</td></tr>
<tr><td>Security classification</td><td>Low risk, general distribution within aviation domain okay</td></tr>
</table>

4.3.2 Impact assessment on Primary Assets

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized	**INITIALISE**	Update	Update	Update
Prioritized	**INITIALISE**	Update	Update	Update

Description	The impact is assessed for the following areas: People, capacity, performance, economic, branding, regulatory and environment. The impact level ranges from 1 to 5, according to the table below. The level chosen by the evaluator should preferably be with respect to European-wide operations but should anyway be explicitly stated. For example, does a capacity impact of '3' (10-30% loss of capacity) refer to an airport, ACC or network level. Being explicit about these assumptions will enable a SESAR-level view of the security risks. It is also necessary to consider the duration of the attack and recovery phase (e.g. an outage of 1 minute is of less concern than one day). For each primary asset 'x', and for each impact area 'y' the assessor must evaluate the following questions: "If we compromise the confidentiality of primary asset 'x' what would be the impact on the impact area "y"?" "If we compromise the integrity of primary asset 'x' what would be the impact on the impact area 'y'?" "If we compromise the availability of primary asset 'x' what would be the impact on the impact area 'y'?" The impact areas are interdependent. For example, a capacity impact has a good chance of having an economic impact and a branding impact. An impact on performance will likely have an impact on capacity. And almost all of those criteria, with the arguable exception of the PEOPLE impact, can be expressed in term of an economic impact. At this stage in the impact assessment, the maximum impact of unlawful interference should be documented. The justification for the impact must be documented with an associated impact scenario explaining the impact.
Examples	

Primary Asset PA#1						
Name: Flight plan validation						
Type: Service						
Description: Area Control Performed in high density airspace above FL285 with limited complexity						
Compromise of Confidentiality						
People	**Capacity**	**Perfo**	**Economic**	**Branding**	**Regulation**	**Environment**
3	1	1	1	1	3	1
Maximum impact: 3						
Operational scenario: Disclosure of military or royal flights is forbidden by law. Disclosure of military or royal flights is forbidden by law. It reveals information on military excerises that should not be disclosed to potential state enemies, and						

may significantly weaken a state's military strategy during military conflicts.

Compromise of Integrity

People	Capacity	Perfo	Economic	Branding	Regulation	Environment
5	4	1	2	3	1	1

Maximum impact: 5

Operational scenario:

1. Discrepancy between FPL in cockpit and the ground ATM systems can lead to conflicts with very late detection, possibly causing a collision. When not causing a collision, but the fault would be known to media, it would still lead to branding damage for concerned airline and ANSP.
2. When many flightplans are compromised, the entire ATM system could not be trusted anymore, causing serious capacity reductions.

Compromise of Availability

People	Capacity	Perfo	Economic	Branding	Regulation	Environment
1	4	1	1	1	1	1

Maximum impact: 4

Operational scenario: If flight plan cannot be validated, the Network Managmenet function does not receive any input at all, and therefore cannot perform its function. This will lead to signficant capacity reductions throughout Europe.

ID	Primary Asset	Confidentiality, Integrity and Availability	People	Capacity	Performance	Economic	Branding	Rgulatory	Environment	Maximum Impact
PA#1	Flight plan validation	**Confidentiality**	3	1	1	1	1	3	1	**3**
		Integrity	5	4	1	2	3	1	1	**5**
		Availability	1	4	1	1	1	1	1	**4**

Tool support: No tool support until further notice

Catalogue

	5	4	3	2	1
IMPACT AREAS	Catastrophic	Critical	Severe	Minor	No impact / NA
PEOPLE	Fatalities	Multiple Severe injuries	Severe injuries	Minor injuries	No injuries
CAPACITY	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss

	PERFORMANCE	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
	ECONOMIC	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income / increased expsenses	No effect
	BRANDING	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
	REGULATORY	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
	ENVIRONMENT	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

Table 1: Primary asset impact assessment table

How to document	**ATM solution projects** • See Medium Risk material sections 1.1 and 1.2 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report" **Enabling solution projects** • See Medium Risk material sections 1.1 and 1.2 "SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.4 Supporting Assets

4.4.1 Identification of Supporting Assets

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		**INITIALISE**	Update	Update
Prioritized		**INITIALISE**	Update	Update

Description	A supporting asset is an entity that helps realise one or more primary assets (i.e. the primary asset would not be delivered or will be delivered in degraded mode if the supporting asset were compromised). Supporting assets possess the vulnerabilities that are exploitable by threats that aim to impair the primary assets, within the scope of the assessment. Whereas the primary assets are intangible services and information, the supporting assets are the tangible entities that enable the storage, processing and exchange of information, as well as the processing and execution of functions or services. When identifying supporting assets consider: • Supporting assets categories include human roles, equipment, hardware and software. • All phases of the lifecycle. Even though SESAR is only covering the initial phases of the lifecycle, security controls and requirements shall be defined for deployment and operational use; • Legacy (existing) systems which will be used in the future (e.g. existing people's roles, hardware or software) shall be included as supporting assets • The transition aspects from today's system to tomorrows • All phases of the Incident preparedness and operational continuity management. To identify supporting assets, or determining whether an entity is a supporting asset, the following questions can be used for each primary asset: • When and how is the primary asset used, by whom and for what purpose? • When and how can the use of the primary asset be interrupted or prevented? • How can a threat or other circumstances interrupt or prevent the use of the primary asset? All primary assets shall be linked with at least one supporting asset, and all supporting assets shall be linked with at least one primary asset. If a supporting asset is not linked with a primary asset it is either irrelevant and can be omitted, or it indicates that the list of primary assets is incomplete.
Examples	• Distance Measuring Equipment (DME) • Ground-based augmentation system (GBAS)

	• ILS • Airline Station Manager • Flight Crew The results of this step and that of the next step are captured together in one table, for which an example is given in section 5.4.2.
Tool support	No tool support until further notice
Catalogue	See "SecRAM catalogue, tab "Supporting Assets". The use of this catalogue is not restrictive, but should be considered as guidance material. To improve best practice in SESAR 2020, after solution level brainstorming new elements for re-use by other projects can be proposed to PJ19 for inclusion.
How to document	**ATM solution projects** • See Medium Risk material section 2.1 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report" **Enabling solution projects** • See Medium Risk material section 2.1 "SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.4.2 Valuation on Supporting Assets

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		INITIALISE	Update	Update
Prioritized		INITIALISE	Update	Update

Description	An attack on a supporting asset may cause one of the impacts on confidentiality, integrity or availability already identified for the primary assets (see section 5.2.2). The valuation on a supporting assets is therefore no more than a refinement of the impact assessment of a primary asset, and explains in more details how a primary asset can be compromised by attacking a supporting asset's confidentiality, integrity or availability. The supporting asset will inhert the impact assessment from the primary asset, as a succesfull attack on a supporting asset will result in a failure or degradation of the primary asset that it supports. Verify that the inherited impact makes sense, and if needed adjust the impact assessment of the primary asset to which the supporting asset is connected.
Example	

<table>
<tr><td></td><td>
<table>
<tr><td colspan="5">Supporting Asset SA#1</td></tr>
<tr><td colspan="5">Name: Instrument Landing System (ILS)</td></tr>
<tr><td colspan="5">Type: System</td></tr>
<tr><td colspan="5">Description: An ILS enables aircraft to land if the pilots are unable to establish visual contact with the runway. It does this by way of transmitted radio signals.</td></tr>
<tr><td colspan="5">Support to:</td></tr>
<tr><td>Precision runway approach guidance</td><td></td><td></td><td></td><td></td></tr>
<tr><td>X</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5">Inherited impacts:</td></tr>
<tr><td colspan="5">Confidentiality: 1</td></tr>
<tr><td colspan="5">Integrity: 5 (People), 4 (Capacity)

An aircraft landing on autopilot with ILS cat III engaged in low visibility conditions may crash if the ILS signal is incorrect. Due to low visibility the pilot may not detect the failure in time.

Once this is known there is on safety issue for any subsequent aircraft, but the runway cannot be used for ILS cat III operations, effectively disabling runway usage during low visibility conditions.</td></tr>
<tr><td colspan="5">Availability: 4 (Capacity)

The runway cannot be used for ILS cat III operations, effectively disabling runway usage during low visibility conditions.</td></tr>
</table>
Table 2: Supporting Asset identification and valuation
</td></tr>
<tr><td>Tool support</td><td>No tool support until further notice</td></tr>
<tr><td>Catalogue</td><td>The impact areas and the severity of impact are defined in this document, section 5.2.2 in the table “Table 1: Primary Asset impact assessment table”. There is no separate catalogue.</td></tr>
<tr><td>How to document</td><td>ATM solution projects

• See Medium Risk material section 2.1 “SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report”

Enabling solution projects

• See Medium Risk material section 2.1 “SESAR 2020 TS-IRS - Template - Part</td></tr>
</table>

	IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.5 Threats

4.5.1 Identification of Vulnerabilities

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	**INITIALISE**	Update
Prioritized		**INITIALISE**	**Update**	Update

Description	Vulnerability refers to the inability to withstand the effects of a cyber attack. All supporting assets may have vulnerabilities.
Examples	

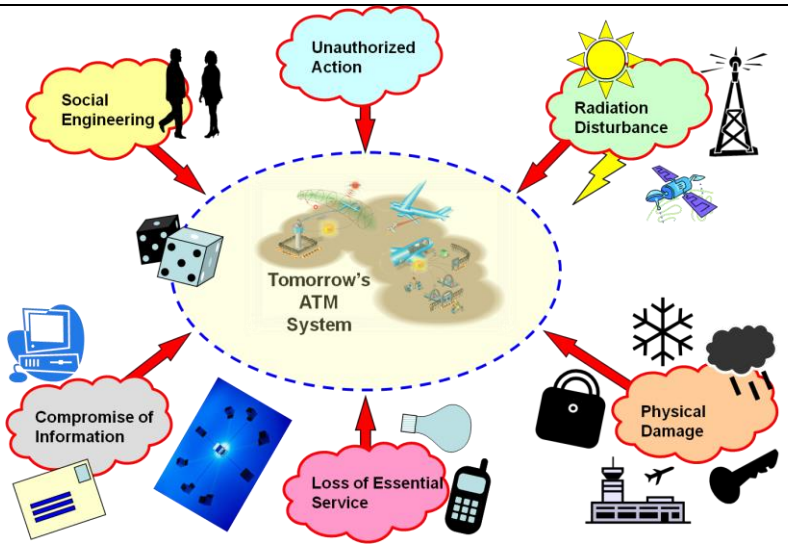
Supporting Asset ID	Vulnerability ID	Vulnerability Description	Vulnerability Exploitation Description
SA#04	V#01	Inadequate protection of cryptographic keys	Unauthorised access to cryptographic keys could lead to fake identity jeopardising data integrity, or to eavesdropping jeopardising confidentiality of data.
SA#01	V#02	Too much authorisations for one person	A disgruntled (former) employee could abuse or damage the system
SA#11	V#03	Lack of validation of the processed data	Service requests with corrupted or fake and incorrect data could cause a system to crash. This is a widely used method to exploit vulnerabilities.

Tool support	No tool support until further notice
Catalogue	See "SecRAM catalogue, tab "Vulnerabilities". The use of this catalogue is not restrictive, but should be considered as guidance material. To improve best practice in SESAR 2020, after solution level brainstorming new elements for re-use by other projects can be proposed to PJ19 for inclusion.
How to document	**ATM solution projects** • See High Risk material section 1.1 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIC - Security Assessment Report" **Enabling solution projects** • See High Risk material section 1.1 "SESAR 2020 TS-IRS - Template - Part IIC - Security Assessment Report"
Security classification	High risk, limited distribution

4.5.2 Identification of Threats

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	**INITIALISE**	Update
Prioritized		**INITIALISE**	**Update**	Update

Description	A threat is a potential cause of a cyber security incident. Threats are independent to controls-in-place and will use vulnerability of a supporting asset to identify a threat scenario. The objective of this step is to identify all the possible threat sources that may attack a supporting asset. A threat is the potential root cause of an unwanted impact. The attacker will attempt to exploit a vulnerability in a supporting asset to achieve their goal. For each threat, the targeted criteria Confidentiality, Integrity and Availability, has to be identified. It connects threats directly to supporting assets and indirectly to the primary assets they support. The process may be performed from different viewpoints: • A vulnerability assessment of all supporting assets to down-select relevant threats. • Attacker view point, e.g. about the preparation time, expertise, knowledge of the target (environment, vulnerabilities, operations etc.), needed equipment of the attacker, possibility of an attack concerning environment, time, feeling to be unobserved (e.g. shiftwork, insider), attractiveness of the target etc and how they can attack a supporting asset, also leading to a set of relevant threats.



Examples

ID	Supporting Asset	Threat	PA#1 Aircraft landing		
			C	I	A
SA#1	ILS	Jamming	1	1	4
		Spoofing	1	5	1
		Eavesdropping	-	-	-
		Phishing	-	-	-
		Vandalism	1	1	4

Tool support

No tool support until further notice

Catalogue

See "SecRAM catalogue, tab "Threats". The use of this catalogue is not restrictive, but should be considered as guidance material. To improve best practice in SESAR 2020, after solution level brainstorming new elements for re-use by other projects can be proposed to PJ19 for inclusion.

How to document

ATM solution projects

- See High Risk material section 1.2 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIC - Security Assessment Report"

Enabling solution projects

- See High Risk material section 1.2 "SESAR 2020 TS-IRS - Template - Part IIC - Security Assessment Report"

Security classification

High risk, limited distribution

4.5.3 Identification of likely Threat Combinations

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	A threat combination is an orchestrated composition of attacks on single vulnerabilities. Cyber attacks are getting more and more sophisticated, being composed of an orchestrated composition of attacks on single vulnerabilities. The aim of identifying the likely threat combinations, is to step into the mind of a skilled and knowleageable attacker and brainstorm on the various combinations of attacks that could lead to a worst case scenarios. A 'Sophisticated' Attack could consist of the following steps: • The adversary knew specifically what application they were going to attack and collected intelligence about their target. • The adversary used the gathered intelligence to attack specific points in their target, and not just a random system on the network. • The adversary bypassed multiple layers of strong defense mechanisms, which may include intrusion prevention systems, encryption, multi-factor authentication, anti-virus software, air-gapped networks, and on and on. • The adversary chained multiple exploits to achieve their full compromise.
Example	

ID	Primary Asset	Supporting Asset / Vulnerability / Threat	Description of the combination
SC#1	PA#01	SA#02 V#01 Th#04	Spear phishing attacks targeting key decision makers in the APOC. Their computers are comprised via an attachment or URL to a compromised website that hosts the malware's payload. Once launched, the malware will try credential escalation and pivoting to gain control over host computers. The infected machines will then map the network and post the results on a Twitter account that acts like a Command & Control
		SA#02 V#01 Th#04	
		SA#02 V#01 Th#04	

				server. To avoid detection, data exchanges between infected equipment will be layer-encrypted in a way that some equipment will act like a proxy without being able to decipher the information. Once the Active Directory is infected, attackers will gain full access to the APOC systems. Mass data can be exfiltrated to be analysed or sold, including operational data relating to flights and intelligence on the airport stakeholders. Finally, the attackers will cover their tracks by destroying the workstations and servers operating the APOC's systems.
				…

Tool support	No tool support until further notice
Catalogue	Not applicable.
How to document	**ATM solution projects** • See High Risk material section 1.3 “SESAR 2020 SPR INTEROP OSED - Template - Part IIIC - Security Assessment Report” **Enabling solution projects** • See High Risk material section 1.3 “SESAR 2020 TS-IRS - Template - Part IIC - Security Assessment Report”
Security classification	High risk, limited distribution

4.6 Risk evaluation and treatment

The security risk is a combination of the impact of a successful attack and the likelihood that the impact will be achieved.

At the end of the risk assessment process a set of risks will have been identified for each supporting asset. These (as illustrated) will state the risk to each primary asset which the supporting asset enables in terms of C, I and A. The risks are categorised as High, Medium or Low. The aim of risk treatment is to reduce the security risk to an acceptable level, by adding security controls.

In order to achieve an acceptable risk level, a number of controls may need to be put in place to reduce the impact. Defence in depth relies on a multi-layered set of unrelated controls acting together to provide protection to a supporting asset through combining different types of controls.

The multi-layered approach to controls means that if one control is compromised then another control should act as the next layer of defence.

> Risk assessment is an iterative process, that needs to be iterated by adding controls untill the residual risk meet the cyber security objectives.
>
> An first iteration of the risk evaluation may be conducted with controls limited to those already in operations (see environmental assumptions, section 5.2) and generic organisational controls (e.g. from MSSC, see footnote on page 11) to ensure focus only on the identification of controls that mitigate risks that do not meet the programme generic security objective.

If the risks cannot be reduced to meet the cyber security objective, the solution architecture needs to be re-considered, or the solution development needs to be withdrawn.

Indicators that architectural changes may be required include:

- unacceptably high residual risks, i.e. a failure to meet security objectives
- a high cost of recommended controls
- the identification of new threats or vulnerabilities
- …..

4.6.1 Identification of Controls

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	A security control is a requirement that increases the protection of a primary (operational) asset against cyber-attacks. A security control may apply to an organisation, a policy, a process, a role, software or hardware. Two types of controls need to be distinguished: 1. Reducing the likelihood of success of an attack by increasing the protection of an asset through the application of controls. 2. Reducing the impact of an succesfull attack by strengthening the contingency measures. By combining multiple controls a stronger defence against an attack is achieved. Best practices can be found in the catalogue. Different controls may be needed to reduce the risk for continuity, integrity and availability. Both existing and new controls need to be identified.
Examples	

<table>
<tr><td></td><td>
<table>
<tr><th>Control</th><th>Supporting asset</th><th>Primary asset</th><th>Baseline / new</th><th>Reduce impact or likelihood</th><th>Rationale</th></tr>
<tr><td>Access rights to ATM secure or sensitive areas shall be regularly reviewed and updated, and revoked when necessary.</td><td>FDP system</td><td>ATC</td><td>Baseline</td><td>Likelihood</td><td>The is considered baseline security for an ANSP</td></tr>
<tr><td>Functional redundancy through a different technology</td><td>ILS</td><td>Precision Landing Navigation Support</td><td>New</td><td>Impact</td><td>The ILS is made functionally redundant by simultaneously requiring GBAS landings.</td></tr>
</table>
</td></tr>
<tr><td>Tool support</td><td>No tool support until further notice</td></tr>
<tr><td>Catalogue</td><td>See “SecRAM catalogue, tab “Controls”. The use of this catalogue is not restrictive, but should be considered as guidance material. To improve best practice in SESAR 2020, after solution level brainstorming new elements for re-use by other projects can be proposed to PJ19 for inclusion.</td></tr>
<tr><td>How to document</td><td>ATM solution projects
• See Medium Risk material section 3.1 “SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report”
Enabling solution projects
• See Medium Risk material section 3.1 “SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report”</td></tr>
<tr><td>Security classification</td><td>Medium risk, controlled distribution</td></tr>
</table>

4.6.2 Impact on Primary Assets after implementation of Controls

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	When strengthening the contingency measures (one of the security control) the impact on a primary asset may be reduced.
Examples	When ILS is made functionally redundand by simultaneously supporting GBAS, the impact on the landing capacity, in case of a succesfull attack on the availability of an ILS, is reduced. The format of the output is similar to the initial assessment without applicaton of controls. See Section 5.3.2 "Impact assessment on Primary Assets", with the addition on the controls now implemented, possibly leading to the reduction of attack impact.
Tool support	No tool support until further notice
Catalogue / Table	Not applicable
How to document	**ATM solution projects** • See Medium Risk material section 3.2 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report" **Enabling solution projects** • See Medium Risk material section 3.2 "SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.6.3 Likelihood of impact on Primary Assets after implementation of Controls

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	In order to evaluate likelihood one may consider looking at the aspects of **exposure**, or frequency of occurrence of the threat source, and **probability of success** of an attack. In order to assess the exposure one could take into account the following considerations from a hacker perspective: • Attention/ attractiveness of the target. This consideration refers to the attention that will attire a successful attack: the economic, cultural, and symbolic importance of the target to society. For example, in case the attention is world-wide, then the attractiveness for the attacker will be high, and the frequency of occurrence (of attempts) of such an attack will be continuous. • Profit. It refers to the potential personal benefits or revenues obtained by

<table>
<tr><td></td><td>the attacker.

• Feeling of impunity. It represents the assessment by the attacker of the likelihood of being identified during the attack (accountability) and the sanctions to which he may be subjected.

• History of threats. To evaluate this parameter, the following questions apply: What has the threat source done in the past, how many times, and was the threat local, regional, national, or international in nature? When was the most recent incident and where, and against what target? A terrorist group is present, assessed to be present, or likely to be active against the system?

• Collateral damage. The potential of the threat to cause collateral damage or disruption to other systems which are not the primary target.</td></tr>
<tr><td>Example</td><td>
<table>
<tr><th>ID</th><th>Threat Combination</th><th>Supporting asset</th><th>Primary asset</th><th>Likelihood</th><th>Rationale</th></tr>
<tr><td>TS#1</td><td>Denial of service attack</td><td>Initial Flight Plan Validation (IFPS)</td><td>Flight Planning</td><td>4</td><td>Interfaces for the IFPS are published on the internet, and therefore a visible target.</td></tr>
<tr><td>TS#2</td><td>Sophisticated attack</td><td>FDP system</td><td>Air Traffic Control</td><td>2</td><td>An attack on an FDP system requires breaches on various security layers, including access to system documentation.</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td></td><td></td><td></td></tr>
<tr><td>TS#N</td><td>Threat scenario N</td><td>Asset Sup_N</td><td></td><td></td><td></td></tr>
</table>
Table 3: Likelihood evaluation
</td></tr>
<tr><td>Tool support</td><td>No tool support until further notice</td></tr>
<tr><td>Catalogue / Tables</td><td>
<table>
<tr><th>Likelihood</th><th>Value</th></tr>
<tr><td>There is a high chance that the scenario successfully occurs in the short term.</td><td>5</td></tr>
<tr><td>There is a high chance that the scenario successfully occurs in the</td><td>4</td></tr>
</table>
</td></tr>
</table>

	medium term.	
	There is a high chance that the scenario successfully occurs during the lifetime of the project.	3
	There is a low chance that the scenario successfully occurs during the lifetime of the project.	2
	There is very little or no chance that the scenario successfully occurs during the lifetime of the project.	1

Table 4 Likelihood scheme

How to document	**ATM solution projects** • See Medium Risk material section 3.3 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report" **Enabling solution projects** • See Medium Risk material section 3.3 "SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.6.4 Residual risk after implementation of controls

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	The security risk is a combination of the impact of a successful attack and the likelihood that that impact will materialize. The impact of a threat scenario is evaluated at two levels: • *The Inherited Impact: this is the automatic impact gathered from the previous information of the threat scenario table. The threat scenarios target the primary assets evaluated on the CIA criteria. By taking the maximum impact of all those targeted criteria, we get the Inherited Impact.* • *The Reviewed Impact (RI): this is an adjustment of the inherited impact due to (a) already implemented (legacy) controls; (b) already planned controls; (c) expert review of impact. The Reviewed Impact relates to reducing the impact rather than reducing the likelihood of attack. The Reviewed Impact is always equal to or less than the Inherited impact. Justification (evidence) shall be provided when the Reviewed Impact is determined to be lower than the Inherited Impact. If the impact is reduced significantly it may be necessary to review the primary assets*

impact assessment.

Residual risks at medium level need to be justified in the security annex. Residual risk as high level is not acceptable.

	Reviewed Impact				
Likelihood	**1**	**2**	**3**	**4**	**5**
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Example

ID	**Threat scenario**	**Supporting asset**	**Reviewed Risk Impact**	**Likelihood** - Value 1-5	**Risk level** (Low/ Medium/ High)	**Justification for medium, if medium**	**Risk Status** Accepted/ avoided/reduced	**Rationale**
TS# 1	Jamming ILS	ILS	4	3	High		Not acceptable	This threat scenario requires additional controls to reduce the residual risk.
TS# 2	Disable electricity	ILS	4	2	Medium	The residual risk for an impact of 4 or 5 by definition cannot be reduced	Accepted	The likelihood has been reduced by requiring independent back-up power supply.

	further than medium.
	Table 5: Risk level evaluation (example)
Tool support	No tool support until further notice
Catalogue / Tables	Not applicable
How to document	**ATM solution projects** See Medium Risk material section 3.4 "SESAR 2020 SPR INTEROP OSED - Template - Part IIIB - Security Assessment Report" **Enabling solution projects** • See Medium Risk material section 3.4 "SESAR 2020 TS-IRS - Template - Part IIB - Security Assessment Report"
Security classification	Medium risk, controlled distribution

4.7 Security requirements

4.7.1 Capturing controls as security requirements

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Non Prioritized		Optional	Optional	Optional
Prioritized		**INITIALISE**	Update	Update

Description	Both the security assumptions identified in section 5.2 and the security controls identified in section 5.6.1 need to be captured as security requirements in the SPR/INTEROP/OSED (ATM solution) and the TS/IRS (Technological solution).
Example	

Identifier	REQ-XXb.YY-SPRINTEROP-UU01.0123
Title	User access management
Requirements	Access to data shall be controlled by applying user access management
Status	in progress

	Rationale	The security control is the output of the solution's corresponding security risk assessment (Annex III of this document)
	Category	Security baseline assumption (from section 5.2) ***or*** Security solution requirement (from section 5.6.1)
Tool support	Not applicable	
Catalogue / Tables	Not applicable	
How to document	**ATM solution projects** • See "SESAR 2020 SPR INTEROP OSED - Template - Part I" chapter 4 for non-technical security requirements (e.g. organisational or procedural). • See "SESAR 2020 TS IRS - Template ATM" section 4.2 for technical systems security requirements. **Enabling solution projects** • See "SESAR 2020 TS IRS - Template EN" section 4.2.	
Security classification	Unclassified	