Security of Air Transport Infrastructures of Europe

D7.9 – Cyber-physical risk analysis

Deliverable Number	D7.9
Author(s)	All Partners
Due/delivered Date	M21/2021-05-12
Reviewed by	ACS, DLR, KEM
Dissemination Level	PU
Version of template	1.07

Start Date of Project: 2019-05-01

Duration: 30 months

Grant agreement: 832969

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969

Document contributors

No.	Name	Role (content contributor / reviewer / other)
1	Matteo Mangini (NIS)	Content contributor
2	Kelly Burke (NIS)	Content contributor
3	Nikos Papagiannopoulos (AIG)	Content Contributor
4	Vasilis Kontothanasis (AIA)	Content Contributor
5	Eric Hervé (ALS)	Content Contributor
6	David Lancelin (CCS)	Content Contributor
7	Thomas Oudin (CCS)	Content Contributor
8	Tim Stelkens-Kobsch (DLR)	Content Contributor
9	Meilin Schaper (DLR)	Reviewer
10	Victoria Peuvrelle (ERI)	Content Contributor
11	Mirjam Fehling-Kaschek (FHG)	Content Contributor
12	Corinna Koepke (FHG)	Content Contributor
13	Georg Trausmuth (FQS)	Content Contributor
14	Hubert Kuenig (FQS)	Content Contributor
15	Luc Sonke (IDE)	Content Contributor
16	Sebastien Clavert (IDE)	Content Contributor
17	Thomas Mauger (IDE)	Content Contributor
18	Nelson Escravana (INOV)	Content Contributor
19	Filipe Apolinário (INOV)	Content Contributor
20	Isabel Praça (ISEP)	Content Contributor

No.	Name	Role (content contributor / reviewer / other)
21	Eva Maia (ISEP)	Content Contributor
22	Alda Canito (ISEP)	Content Contributor
23	Marcin Przybyszewski (ITTI)	Content Contributor
24	Ioannis Chasiotis (KEM)	Content Contributor
25	Eftichia Georgiou (KEM)	Content Contributor
26	Livia Torterolo (NIS)	Content Contributor
27	Gabriele Guasco (NIS)	Content Contributor
28	Antonis Kostardis (SAT)	Content Contributor
29	Leonidas Perlepes (SAT)	Content Contributor
30	Aggelos Aggelis (SAT)	Content Contributor
31	Robert Sabo (SAV)	Content Contributor
32	Milan Rusko (SAV)	Content Contributor
33	Marian Trnka (SAV)	Content Contributor
34	Marcella Scuccimarra (SEA)	Content Contributor
35	Elena Branchini (SEA)	Content Contributor
36	Francois Déchelle (TLB)	Content Contributor
37	Maja Despot (ZAG)	Content Contributor
38	Marin Tica (ZAG)	Content Contributor
39	Marko Licina (ZAG)	Content Contributor
40	Sven Hrastnik (ZAG)	Content Contributor
41	Vasileios Kazoukas (KEM)	Reviewer
42	Meilin Schaper (DLR)	Reviewer

Document revisions

Revision	Date	Comment	Author
V0.1	2020-11-19	Final draft for public version based on D2.3	NIS
V0.2	2021-01-18	Sensitive content removed/altered	ALS, DLR
V0.3	2021-01-19	Sensitive content removed/altered	AIA
V0.4	2021-01-20	Figures 2.4 and 2.5 updated for better quality	INOV
V0.5	2021-01-20	Sensitive content modified for PU version	SEA
V0.6	2021-01-20	Scenario descriptions added for Athens	NIS
V0.6	2021-01-28	Initial security check and change requests	Vasileios Kazoukas
V0.6	2021-01-28	Initial quality review	Meilin Schaper
V0.7	2021-02-01	Updates according to reviews	INOV, NIS
V0.7	2021-02-02	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-02-02	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

This document provides a report on the cyber and physical threat scenarios typical of attacks that threaten airport infrastructures and the results of a risk analysis applied to these scenarios. No risk analysis results are reported here to maintain the safety of airports.

First a section is presented that describes the five threat scenarios (two for Athens, one for Milan and Zagreb, and one for the simulation scenario of DLR) by integrating the information collected during the activities of task T2.2 and during the focus group meetings held at each airport site. This core activity was also carried out by collecting interviews aiming to describe the threat scenarios in a realistic and effective way. The interviews provided a snapshot of the current situation on behalf of security measure application at the airport sites. The identification of cyber and physical threats and their representation in a context of assets, vulnerabilities, probability of occurrence, operations and security controls conclude the first part of this document and prepare the basis for the project activities of most of the following WPs. Only a simplified version of the threat scenarios are included here so as not to potentially indicate any vulnerabilities in airport environments.

In parallel a methodology for risk analysis was studied, analysing the state of the art and integrating this with the knowledge and expertise of the project partners. This activity led to the identification of a custom methodology, according to the EU Cybersecurity Strategy, the NIS directive and ISO31000 guide lines, to be applied to the airports' critical infrastructures and to the use of a dedicated tool (RIS) to configure and perform the risk analysis of the five threat scenarios.

There is a detailed description of the risk analysis methodology used, including the scope of the assessment, the players involved, the elements which serve as input and the outcomes produced. The innovative configurations specifically made for SATIE to the risk assessment approach are described in detail, particularly emphasizing RIS' unique ability to be tailorable and to analyse both cyber and physical threats and vulnerabilities.

Finally, while the results of the risk analysis performed on each scenario is not possible for public dissemination, the outcome of the current deliverable was used by other tasks of the project (i.e. T2.4, T3.1, T6.1 and T6.2) as a baseline and a reference with concerns to representation of threat scenarios and the outline of risks for each airport site.

At the end of the deliverable, there are multiple annexes listing the threats, vulnerabilities, and security controls included in the risk assessment. These are specific to the RIS methodology and reflect some of the configuration changes made for SATIE.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ABC	Automated Border Control
AC	Access Control
ACTO	Air Traffic Controller Operator
AIAA	The American Institute of Aeronautics and Astronautics
ANSSI	National Cybersecurity Agency of France
AOCC	Airport Operations Control Centre
AODB	Airport Operation Database
AOS	Airport Operation System
API	Advance Passenger Information
APIS	Advance Passenger Information System
ARINC	Aeronautical Radio, Incorporated
ATC	Air Traffic Control
ATM	Air Traffic Management
ATR	Automatic Tag Reader
BHS	Baggage Handling System
BPM	Baggage Processed Message
BRS	Baggage Registration Services
BSM	Baggage Source Message
CARVER2	Criticality Accessibility Recoverability Vulnerability Espyability Redundancy
CBRN	Chemical Biological Radiological and Nuclear
CCTV	Closed-circuit television
CMMS	Computerized Maintenance Management System
CSP	Cloud Service Provider
DCS	Distributed Control System
DMS	Demilitarised Zone
DoS	Denial of Service
EBIOS	Enterprise Building Infrastructure
EBIOS	Expression of Needs and Identification of Security Objectives

Acronym	Definition
EDS	Explosive Detection System
EMS	Electromagnetic Interference
ENAC	Italian Civil Aviation Authority
ENAV	Italian Air Navigation service provider
ENISA	The European Union Agency for Cybersecurity
eth.	Ethernet for the PLC
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FIDS	Flight Information Display System
GDF	Guardia di Finanza
GDPR	General Data Protection Regulation
GLPI	Gestionnaire Libre de Parc Informatique
gtw	PLC gateway
HMI	Human-machine interface
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information and Communications Technology
ID	Identification
IEC	International Electrochemical Commission
IED	Improvised explosive device
io	Remote I/O for the PLC
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
M-AIS	Milan Airport's Information System
MITM	Man-in-the-middle
MSP	Managed Service Provider
N.A.	Not Applicable

Acronym	Definition
NIS	Network and Information Security
NSA	National Security Agencies
NSAC	National Security Advisory Centre
NTP	Network Time Protocol
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OES	Operators of Essential Services
OS	Operating system
OT	Operational Technology
PA	Public Announcement
PAC	Programmable Automation Controller
PDCA	Plan-Do-Check-Act
PLC	Programmable Logic Controller
RIS	Risk Integrated Service
RMS	Resource Management System
RTCA	Radio Technical Commission for Aeronautics
RTU	Remote Terminal Unit
SAC	Sort Allocation Computer
SATIE	Security of Air Transport Infrastructures of Europe
SCADA	Supervisory Control and Data Acquisition
SecRAM	Security Risk Assessment Methodology
SECUR-ED	SECure URban Transportation – a European Demonstration
SES	Single European Sky
SESAR	Single European Sky ATM Research
SITA	Société Internationale de Télécommunications Aér
SMS	Security Management System
SOC	Security Operation Centre
SSL	Secure Sockets Layer
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege
SWIM	System Wide Information Management

Acronym	Definition
UFIS	Universal Flight Information System
UI	User interface
ULD	Unit Load Device
USB	Universal Serial Bus
VBIED	Vehicle Born Improvised Explosive Device
VHF	Very High Frequency
VIP	Vulnerability Intelligence Platform
VPN	Virtual Private Network
WP	Work Package
XML	Extensible Mark-up Language

1 Introduction

In this deliverable the activities and the results of SATIE´s task T2.2 “Scenarios of threat and cyber-physical risk analysis” are documented in detail but without any of the sensitive information. The results are relevant for the two main objectives of the task, which are the identification of the scenarios of threats and the execution of a risk assessment and analysis on them using the Risk Integrated Service (RIS) tool. The outcomes of this deliverable will be used to feed the work packages to be followed as a baseline of the entire simulation platform design and all implementation activities. Therefore, it is crucial to gather reliable and realistic information from all the partners involved in the project and, in particular, from the end-users which, with their expertise, can contribute to and support the definition of the scope of the assessment as well as of the baseline for the simulation and demonstration environments. Furthermore, risk assessment in general represents the baseline on which a Security Management System is based. This is even truer in a complex cyber-physical eco-system such as an airport, one of the critical infrastructures with the highest rate of cyber and physical potential attacks, where security, cybersecurity and safety are tightly correlated.

Scenarios of threats are defined with the contribution of end-users and stakeholders, identifying a background of threats and vulnerabilities that are typical for attacks that threaten airport infrastructures. The main elements which describe a specific subset of the whole airport system, made up of operations, assets, threats, vulnerabilities and security controls, are configured in the RIS tool. Moreover, the interrelations among elements making up the scenarios are considered and a custom methodology is developed, implemented in RIS and applied to evaluate and analyse the risk in the scope of the five threat scenarios. An important and characteristic aspect of this assessment is the inclusion of cyber and physical assets, threats and vulnerabilities, representing parts of the airport operations, which are identified for the scenarios in a comprehensive view. At a first glance, according to the EU Cybersecurity Strategy and the Network and Information Security (NIS) Directives, airports receive useful information for their prevention and preparedness phase, containing information about which security measures deserve an implementation effort, where the most vulnerable slices of the organization are, which assets have a higher level of risk and which threats can affect them, causing the worst risks for the overall systems.

In this task a lot of security constraints have to be taken into account: handling critical and sensitive information for the airport operations requires an EU-RESTRICED classification level of the deliverable. Specific procedures are then implemented to treat and exchange data, software and documents used and produced in this task in a proper and secure way, following the guidelines and the constraints of the EU and of the single National Security Agencies (NSAs).

The elaborated results not reported here were shared with the end-users and with all partners in the project so that they could help to further address custom and technical analyses for prevention, detection and mitigation of threats in the airport context. The threat scenarios will be used to lead the design and development of the interoperable toolkit of SATIE. This will be achieved together with the elements and attributes that characterize them. This set up provides active support to airport operators and cooperation among different stakeholders, as well as the validation process of the overall platform. In fact, the results of task T2.2 will be an input for subsequent tasks T3.1 “Assets management against cyber vulnerability breaches”, T4.1 “Systems interoperability and log semantics”, T5.2 “Investigation system with time series analysis of multistep threat scenarios”, T6.1 “Preparation of and integration on simulation platform”, T6.2 “Test, verification and validation” and T7.3 “Best practices for updating airport security standards and policies”.

2 Background and scope

The five pilot scenarios of threat are described here to create the agreed-upon conceptual framework for the risk assessment to be performed. The five scenarios cover different areas of airport infrastructure but they cover all major airport operations when seen as pieces of a greater puzzle. Importantly, these distinct scenarios give us five unique points of view on airport infrastructure and on the possible complexities of such attacks in the transport sector. Therefore, for each scenario, a different aspect is explored in further detail. The topics that are deeply analysed in the context of a specific scenario include “social and human impacts” (section 2.1.2), “anomaly detection” (section 2.4.2), “business implications of command-control systems” (section 2.4.3), “cyber-physical dependencies” (section 2.2.2) and “analysis of past cyber-attacks” (section 2.5.3).

Behind this project there is a call that has specifically identified a gap in the security market: the need for a solution preventing, detecting, avoiding or mitigating combined physical and cyber threats (1). The decision that the partners took while building the proposal was to demonstrate that the SATIE solution would not only have constituted a novelty on the market, but the best new solution on the market. To realize this ambitious aim, the partners agreed that the prevention of a bomb attack would have been too easy, and consequently decided to build up different scenarios-situations according to each airport, based on the end users’ knowledge of their airports. Decisions made not only took into account operations manuals, but even airport layouts.

The partners considered that the more the attacker knows the details of the site they are attacking, the more serious the results will be. The echo of the attack will be proportional to a series of parameters, including how deep the attack reached and how much deeper the same attack could have reached. This is why the SATIE solution has been designed and built to have different modules that can be adapted to each different customer’s (airport’s) needs, according to the sensitivities of the areas chosen, which is in the exclusive knowledge of the customer (airport) itself. Understanding known vulnerabilities at the airports can help with the risk assessment to determine how to address those vulnerabilities. However, due to limitations and the need to preserve the safety of the aviation industry, no known vulnerabilities will be presented in this document.

The following sections, besides describing in very general terms the initial drafts of each scenario, offer some justification for why each end-user selected a particular scenario to make the attack both complicated (to test the solution) and, at the same time, realistic (in accordance with their rules and layouts). As discussed in extensive detail in section 2.1 in SATIE deliverable D6.2 (2), there have been many attacks or incidents which have occurred in the past, specifically targeting critical airport systems. There have also been physical attacks against aircraft, such as the bomb explosion of Metrojet Flight 9268 in October 2015 (3).

In the near future, it is most likely that many cyber-physical attacks will emerge against airport systems. The earliest known example of a cyber-physical attack dates back to 2010 and was Stuxnet, a malware that was employed to derail the uranium enrichment process at Iran's Natanz nuclear facility by sabotaging centrifuges. The malware infected PLCs and was designed to target only Siemens SCADA systems that were used by the Iran nuclear program (4). There are many reasons why some attackers will combine cyber-attacks and physical attacks in order to achieve their goal.

First, the cyber vector can be used to amplify attacks to affect the physical world more significantly. Second, the combination of cyber and physical attacks can also be used to increase the probability of success of an attack by disorganizing security operators, overburdening the airport staff, creating a diversion, etc.

Third, security measures and means prevent the emergence of physical threats against airports and aircraft. Since the 9/11 attacks, there have been physical security improvements in all airports. For example, the majority of airports around the world have implemented baggage screening directly into BHS systems: all the bags are analysed by Explosive Detection System (EDS) machines.

Fourthly, airports are considered Operators of Essential Services (OES). Thus, in some countries, they are obliged by directives and regulations to apply security rules to their essential information systems.

2.1 Scenario #1 – Athens airport

For the scenario to be as realistic as possible, we conducted interviews during the scenario definition phase with the cyber and physical experts about the applicable and anticipated cyber and physical threats, risks and actions that are possible at an airport environment. Furthermore, during this phase, we reviewed real cyber and physical security incidents that have occurred at major airports in the past. Following this preparation work, we came up with a multistep scenario that includes both cyber and physical attacks, in order to depict the strong correlation between these types of threats.

In this respect, the scenario aims to create confusion among passengers, disruptions to airport and airline operations and distractions of the airport's cyber and physical response teams that will try to mitigate the impact and respond to the attack. The attack on the airport's IT systems will act as a decoy to create confusion to passengers and airport personnel and keep the physical and cyber access control security practitioners at the airport engaged so they can perform the main target of the attack which has maximum impact on passenger safety.

For one to better understand the magnitude of the potential impact that such an attack can cause, some statistics can help. During a busy day at the airport (i.e. during peak summer periods or Christmas, etc.), the airport processes more than 110,000 passengers, while at given peak periods within such days, there are up to 30,000 people present in the airport terminal, including people that accompany passengers as well as airport staff.

One can estimate what the effect and impact of such an attack could potentially be in terms of loss of human lives and damages and the long-lasting effects in the aviation industry.

2.1.1 Scenario #1 - concept

This threat scenario involves two unsuspecting cyber-attacks to the FIDS and AC system, to gain enough information to be able to control the movement of people and stage a sure-fire physical attack in the parking lot area. The mitigation of the two cyber-attacks also occupies the airport's security response teams increasing the probability that the subsequent physical attacks become a devastating success.

2.1.2 Social and human impacts

This scenario involves major confusion for the passengers as they cannot locate the right check-in areas, departure gates, or correct baggage carousels. It also causes the overwhelming of employees as they are similarly unable to properly direct passengers. While doors to secure areas have been opened, staff would not be able to control and block unauthorized people from entering. All this stress for the passengers and employees would potentially have significant psychological effects. Similarly, the fact, that data could be leaked including sensitive data, which would jeopardise GDPR regulations, may cause stress. These data breaches, mayhem, and unauthorized accesses could cause financial repercussions as well.

The definition of terrorism itself is disputed and multidimensional, in Title 22 of the U.S. Code, it is described simply as politically motivated violence perpetrated in a clandestine manner against non-combatants (5). Nevertheless, whether to classify an event as terrorism or another type of warfare depends on the interpretation of its motives, as there are morally- and legally-diverging perspectives on how to interpret terror attacks. Thus, a terror attack like the one described above is not simply meant to provoke fear and chaos among passengers, but will have other ulterior motives which can be ideological and/or economical. This is because the impact of a terror attack is never only contained to the on-site destruction, but has overarching consequences. Such consequences are investigated in the next paragraphs.

The most immediate impact of this scenario on passengers is physical injury due to possible mass panic, resulting in stampedes and other possible physical injuries due to mass human movements. The second direct impact on humans present during the scenario is the immediate mental impact: distress, stress, terror and other such feelings. These feelings can have a snowball effect and increase the risk of further physical injury. Further down the line, this attack can cause lasting mental disorders due to the mental strain endured during the attack, the most frequent being the development of post-traumatic stress disorder.

As previously hinted, the consequences of terrorist attacks are not restricted to the immediate impacts on the victims and economic cost of the possible physical destruction which can occur during the attack. Terrorist attacks have societal and financial impacts which go much beyond the event. In fact, such events can, among others, increase nationalism and foreign scepticism if the attack was carried out by a foreigner. This in turn can have lasting negative consequences for foreigners and religious minorities regardless of their nationality, leading to further discrimination and stigmatization. Depending on how close the attack would be to an election, a consequence could be a shift of public opinion on the local and/or national government.

The attack could also have legal or political consequences, leading to the enactment of laws which heighten security requirements at airports and other critical infrastructures. This would affect any airports and could potentially lead to further security issues at other airports during the transition period.

Another potential effect is financial: beyond the initial direct economic losses due to physical destruction at the airport, terrorist attacks can make markets more uncertain as investors might refrain from investing in a non-safe environment (6). As such, an appropriate crisis management response is crucial. The same logic applies to trade in general, and the airport might lose carriers that will choose to use another airport for their cargo. Tourism in general in the region or the country might suffer if potential travellers feel unsafe in coming to the country as a consequence of the terrorist attack (7).

Lastly, the scenario poses an issue from a data protection perspective, as the attack could compromise the physical safety of systems which contain personal data, due to the overburdening of staff. Intruders could take advantage of the confusion and physically access sensitive information.

2.2 Scenario #2 – Athens airport

This threat scenario was designed to include physical and cyber-attacks. The scenario starts with a compromised employee managing to get access to the airport's critical systems. The role that compromised employees play in the vulnerabilities of all sizes of corporations is massive and growing. In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by compromised employees (8). Also, the specific type of threats will be one of the key threats that will dominate the 2040 landscape in air transportation (9). Furthermore, in the most recent report published by The European Union Agency for Cybersecurity (ENISA), it is stated that the average annual cost of cybersecurity incidents caused by an insider to the organisation is estimated around €11.45

million (10). A detailed list of real past attacks performed by compromised employees is included in deliverable D6.2, in section 2.1.1 and 2.1.2 (2).

Based on the review of past incidents, there are many real incidents where authorized personnel used their privileged physical access rights to carry out terrorist attacks and in some real past incidents they collaborated with attackers. In addition to this and as further described below the cyber-attacks against the critical systems aim to create panic in the crowd. Even if the terrorists do not succeed to place the bomb or the announcement is a hoax, the stampede of the crowd could lead to many injuries as happened during the Oxford circus tube station incident where 16 people were injured after a false report of gunfire led to a mass panic in the station and surrounding streets (11).

2.2.1 Scenario #2 - concept

Malicious airport personnel have become an increasing threat at airports. This threat scenario is performed by a group of three two attackers and includes a corrupt employee exploiting their privileges, which allows for a cascade of threats and events. By the corrupt employee allowing malicious access to the police database, the entrance of passengers onto EU soil is tampered with, allowing terrorists to enter undetected. Not only that, but further cyber-attacks to the police border control cause crowds, confusion, and overburden police officers who must resort to manual checking and overriding. This combined cyber-attack potentially results in countless, devastating future attacks on EU soil.

2.2.2 Cyber-physical dependencies

The role that compromised employees play in the vulnerabilities of all sizes of corporations is massive and growing. According to a report from Ponemon Institute, the number of insider-caused cyber security incidents increased 47% since 2018, while the average annual cost rose by 31% (8). Also, the specific type of threats will be one of the key threats that will dominate the 2040 landscape in air transportation (9).

This scenario involves a very clear demonstration of how a cyber-attack can turn into a physical attack and also trigger other cyber-attacks. This scenario clarifies how the cyber assets and physical assets within the airport environment are closely interconnected and can affect each other. While airports tend to maintain schematics of their systems, these are often segregated. However, as this scenario demonstrates, a more exhaustive mapping of all cyber and physical assets would be much more helpful in being able understanding and predicting how threats and negative impacts can propagate through the airport infrastructure.

2.3 Scenario #3 – Milan airport

The Milano scenario was designed to include physical and cyber-attacks. The combination of a cyber and physical attack happening simultaneously makes the attack more difficult to be detected. For the project purposes, the attacks have been conceived to happen in the same location.

It is very important here to underline that no airport in the world is equal to another and that every airport is a small city which has its own peculiar design that depends mostly on its geophysical characteristics and on its possibility to expand further in the future. The peculiar design of each airport makes some locations inside it more sensitive (at risk) than others, in spite of the border between airside and landside. This is why all the people holding an airport badge, during the training courses for the release of the badge, are very well explained that they must consider themselves responsible for the security of the airport. Not only the security personnel or the people of the Operations Department: everyone holds part of the responsibility for the fact that they accept and hold the badge,

they all must have an attentive eye and refer in case they see something wrong or if they consider that what they see might put anything or anyone at risk (“see something, say something”).

As said at the beginning of this chapter, the location taken into consideration for the physical attack is also the one where the cyber-attack will take place. It is the place where people are in charge of the following activities:

- Resource scheduling on a seasonal or daily basis.
- Assignment of stands, gates, check-in desks, baggage claim carousels and carousels/piers for departing luggage.
- Information to the "*airport world*" of the airport's operational situation.
- Monitoring of information systems.
- Supervision and control of all airport processes, both terminal and apron (from inside the control room and from the terminal).
- Safeguarding and guaranteeing equal operating opportunities.
- Regularity of airport operations.
- Emergency management.

For the purposes of the project, the target of the cyber-attack that infects the PC in this selected location is the system responsible for assigning the aircraft stands, gates and for the information displayed to the public. Below is a general description of how this scenario unfolds.

2.3.1 Scenario #3 - concept

The Milan scenario targets a specific location. The scenario immediately starts with a cyber-physical attack on the security doors’ card readers with falsified information allowing access to the unauthorized person(s). The unauthorized person(s) gains access to the location through a security door spoofing the card reader. This unauthorized access possibly endangers the authorized personnel in the secure areas and the closed-circuit television (CCTV) system if it is altered so that it won’t record the intruder’s entry. The intruder can then threaten to take the people in the location as hostages, thus generating panic and paralyzing the operations.

The other attack is by a hacker acting under the command of a terrorist: thanks to an undetected social engineering attack that infects one of the PCs of this selected location. They initiate a cyber-attack on the airport system that distributes information to stakeholders and passengers. This attack can ultimately lead to the alteration of the information to be displayed to passengers.

Besides compromising the system that displays information to the passengers, to generate more confusion, the hacker, under the terrorist’s command, proceeds with a cyber-attack to the system regarding the boarding gate assignment. This then affects all passengers trying to find the proper gate, causing mayhem. Another system is attacked to modify the apron parking assignments, which is another good way to create confusion.

Finally, there is a physical attack to the electrical, phone and radio systems, which are essential for normal activities and fundamental in case of emergency.

As a conclusion, this scenario focuses on a cyber-physical attack performed in a specific location and on some systems used in this location. The increased difficulty to alert the first-responders worsens the scenario.

2.4 Scenario #4 – Zagreb airport

This threat scenario is unique in that it unfolds within one airport operation – the BHS – but it similarly includes both physical and cyber-attacks and involves all BHS operations. In the following a complete description is provided.

Along with the SATIE project, Scenario #4 was modified and developed in parallel. It was originally conceived that social engineering would be conducted on a member of the BHS team, but this was rejected as an unlikely or hardly justified event. Based on the research of past attacks (see section 2.5.3 which is expanded upon in deliverable D6.2 (2)), it seems more realistic that the attacker appears in the form of a corrupted BHS maintenance operator. His motives can be various: from the money demanded in the first mini-scenario, to dissatisfaction with work and revenge on the employer through the second mini-scenario, to religious or political beliefs in the last. All three mini-scenarios or storylines are briefly described in section 2.4.1.

Although attacks on the BHS may have not occurred yet or at least were not publicised, it does not mean they could not happen. An objective of SATIE is to anticipate future attacks which may occur. The fact that the BHS seems bulletproof, means that it can be easily targeted because everyone is confident and acts careless. Since the location of BHS and its core is on the airside of the airport, it has limited and restricted access rights. This part of the airport is covered by safety management, where all safety-related anomalies and incidents are reported in order to determine the precursors of accidents or potential safety hazards. Examples of significant safety occurrences are listed in the airport's safety management manual. Because of this and strict airside access control and security inspections of personnel, it is hard for an outside attacker to reach the BHS area. In addition, the airport has implemented an identification (ID) card system that grants protected area access to persons and vehicles.

2.4.1 Scenario #4 - concept

This scenario is divided into three storylines where both cyber and physical attacks are combined. The BHS at the airport is under attack in all of the mini-scenarios, which leads to disorganized baggage handling service and potential threats to the aircraft and human lives. Common to all attacks is that they begin from within, initiated by a corrupt BHS employee.

The first mini-scenario, "Ransomware", is easily feasible if an attacker has BHS area access. Starting from a USB device inserted in any BHS workstation, the malware spreads through the network and attacks SCADA which ultimately ends with an inaccessible BHS and the impossibility to sort passengers' bags. The attacker's motive is money and it is expressed by asking for a ransom to return everything as it was. By this turn of events, passengers may be most affected indirectly: although their safety is not compromised, the denial of baggage service will probably lead to delayed flights or lost bags. On the other side, Baggage Registration Services (BRS) employees who should scan the bags will become disorganized and be put under intense pressure to complete their job on time under extraordinary circumstances. Since the BHS area is equipped with potentially dangerous vehicles and devices, safety at work could be compromised and injuries become more possible.

The second storyline, "The Lost Baggage", leads to similar consequences as described above. It will be a bit harder for the attacker because it requires physical access to a particular part of the BHS system which is in a highly protected and monitored location. However, a corrupt employee can pretend to have some actual work on that part and connect a Raspberry Pi to a port on the BHS system. This will cause confusion in the BHS area where all the bags will be sent to the manual coding station. Human errors are easily possible there because all bags need to be scanned manually and allocated accordingly. Undoubtedly a certain amount of baggage would remain unloaded into the aircraft and reported as lost at the airport of departure.

2.4.2 Anomaly detection

The mini-scenarios described in Section 2.4.1 are centred on the disruption of the BHS by possibly letting dangerous baggage to enter the system. A piece of baggage can be dangerous if an anomaly is detected inside it, but a full anomaly detection process is time consuming and usually performed by a human. The danger of baggage can be extended to its owner or the absence of an owner. To avoid

potentially dangerous normal baggage entering the BHS, it is important to check if anomalies are present in passenger data (e.g. a black-listed person, anomalies in the reservation and/or payment processing, advanced profiling, etc.) as soon as check-in occurs to detect potentially suspicious baggage. In addition, as traceability between baggage and their owners is made through a physical token (i.e. the sticker placed on the baggage) that can be deteriorated voluntarily or by poor handling of the baggage, it is important to be able to reinforce this single link. Therefore, a novel approach is to use visual recognition algorithms to register baggage and link it with a passenger. This allows the identification of the bag's owner in those cases of physical token alteration, thus reducing the loss of information on potentially suspicious baggage.

In case of a physical intrusion detection in a critical airport area, this approach could be used in multiple cases and scenarios. Even if the BHS is totally protected against the intrusion of suspicious baggage or a cyber-attack, this is useless if a suspicious individual can access it. This kind of intrusion can happen when the suspicious individual follows an authorized individual, using coercion to gain access or even steal their credentials. The addition of biometric access controls to critical airport areas grants assurance that only individuals with correct credentials can access critical zones. The use of video will allow a non-invasive biometric identification to validate the ownership of the access token used to access the zone and facilitation of airport area access. When a group of individuals tries to access a zone using only one token in the group, the owner will be identified as the owner of their token but all other individuals entering the zone with them will also be captured on the video. Verifications can be made without validating their physical tokens, consequently. If any unknown individual tries to access the zone or use abnormal behaviour such as coercion or shadowing of a token owner, an alert will be sent or the access will be denied even if the token is valid.

2.4.3 Business implications of command-control systems

This scenario focuses on an attack on the BHS, but not just a physical attack, it includes cyber-attacks to the ICS and SCADA. These systems control the coordination of the BHS. And therefore, any attacks on or detriment to these systems have serious implications for the airport as a business. As previously described in D2.2 (12), BHS are ICS mechanisms deployed in airports that ensure all the necessary operations to guarantee baggage dropped off at airport check-in areas are delivered securely to the destination planes (also known as the baggage handling lifecycle). An example BHS, illustrated in Figure 2.1, is an ICS composed of the following main classes of technological devices:

1. Physical assets – these are the core business of the transportation infrastructure and deliver a broad type of services to end-users that rely on the activities of these organizations (i.e. passengers and airline companies). This example BHS uses conveyors (including mergers, diverters, and pushers), EDS, baggage scales, ATRs, CCTV and cameras.
2. Modular units – these are intelligent embedded devices that serve as an interface between physical and digital assets of the ICS organization. With the possibility of functioning as sensors or as actuators, these technological components are directly connected to physical assets (wired) and can collect information about the asset's physical state (acting as a sensor) and manipulate them according to certain events received from ICS control units (acting as an actuator).
3. Control units – these are logical computing devices[1] connected to the modular units that decide, based on the input information gathered from modular sensor units, the actions that should be carried out by the actuator units to guarantee one or more airport services. Such decision capabilities are loaded as low computational programs[2] each implementing one or more airport

[1] Some examples of control units used in airport ICS are PLC, Remote Terminal Unit (RTU) and Programmable Automation Controller (PAC).

[2] Most control unit programs are developed in IEC 1131 or IEC 1499 programing languages (first one is used for centralized control unit, while the other one is used for distributed control units).

service. Moreover, contrary to modular units that only communicate with one control unit, control units can also be connected[3] to a wide range of IT devices present in the ICS network. In this way they collaborate by exchanging high-level information of the services provided by the airport. In this example BHS, programmable logic controllers (PLCs) are used as control units and the level of collaboration between these control units follows a Distributed Control System (DCS), where more than one central control unit is used to provide all airport services.

4. Human-machine interface (HMI) – are IT devices that serve as entry points for airport staff to interact with the ICS system. In this BHS, the computers of the manual coding station, the tele-maintenance workstation, and the Computerized Maintenance Management System (CMMS) implement this desired functionality.
5. Sort Allocation Computer (SAC) system – this controls all baggage processes, namely tracking, sorting and storage management. It connects directly to Airport Operation Systems (AOSs) and to airline check-in software, to extract information about flights and baggage using standard messages: Baggage Source Message (BSM) and Baggage Processed Message (BPM). The SAC sends sortation decisions to BHS control units.
6. SCADA – these are IT devices that supervise the work performed by the control units that comprise the ICS.

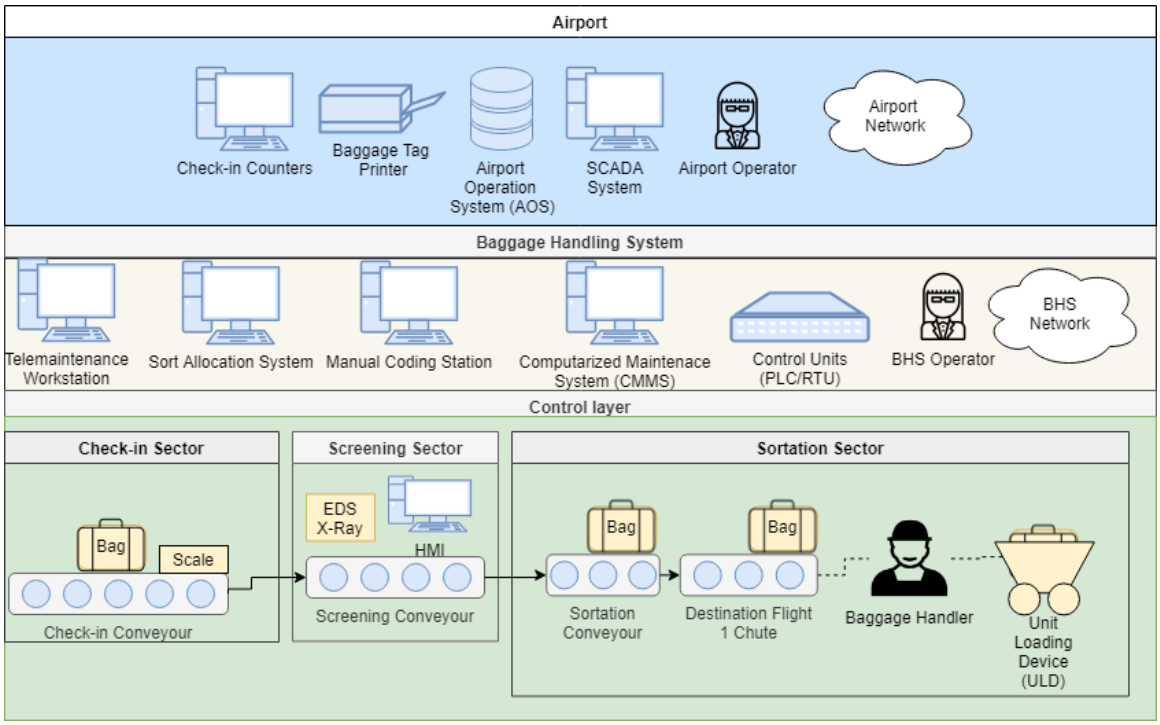

Figure 2.1: An example BHS distributed control system architecture

The services offered by the BHS include: baggage check-in (which checks baggage authorizations to be boarded to the assigned plane, weights and emits the baggage tag), baggage reconciliation (delivers baggage from the airplane to the passenger), baggage screening (which checks for potential evidence of explosive material objects inside the baggage), baggage sortation (which separates baggage received on BHS according to the destination flight to allow the easy distribution of baggage by plane), baggage tracking (that monitors the route taken by each baggage from check-in to the destination plane), baggage handling (which involve loading sorted baggage from the conveyor to the unit loading devices), baggage transportation (which involves the assurance that checked baggage reach assigned

[3] Central units can connect to other IT devices using two types of network protocols: fieldbus protocols; and Ethernet protocols. Most common fieldbus protocols in ICS are: Modbus; Controlnet; profibus. Most common Ethernet protocols are: Profinet; Ethernet/IP; etherCAT.

aircraft), BHS monitoring & management operation (which monitors the BHS behaviour, detects service malfunctions and produces alarms).

The BHS services are accomplished by the following components/entities:

- All BHS operations – involve airport operator, airport operation database, baggage and SCADA (**actors**) and gateway control network switch (**components**).
- Baggage check-in operation – involves airlines, passenger (**actors**) check-in conveyors, ATR, baggage scales (**components**).
- Baggage reconciliation operation – involves Baggage Reconciliation System (BRS), airlines, passengers (**actors**) and sortation conveyors (**components**).
- Baggage screening operation – involves BHS operator, airlines, passengers, police (**actors**) and screening conveyors, screening PLC, screening HMI, EDS (**components**).
- Baggage sortation operation – involve: BHS operator (**actor**), the SAC, airport operation database, sortation control units, diverters/pushers, merger, Manual Coding Station (**components**).
- Baggage tracking operation – involves BHS operator (**actor**), CCTV, tracking control units, ATR (**components**).
- Baggage handling operation[4] – involves Baggage handler (**actor**), sortation conveyers (**components**).
- Baggage transportation operation– involves Baggage handler (**actor**), transportation PLC (**component**).
- BHS monitoring & management operation – involves BHS operator, BHS maintenance (**actor**), CMMS, and a tele-maintenance workstation (**component**).

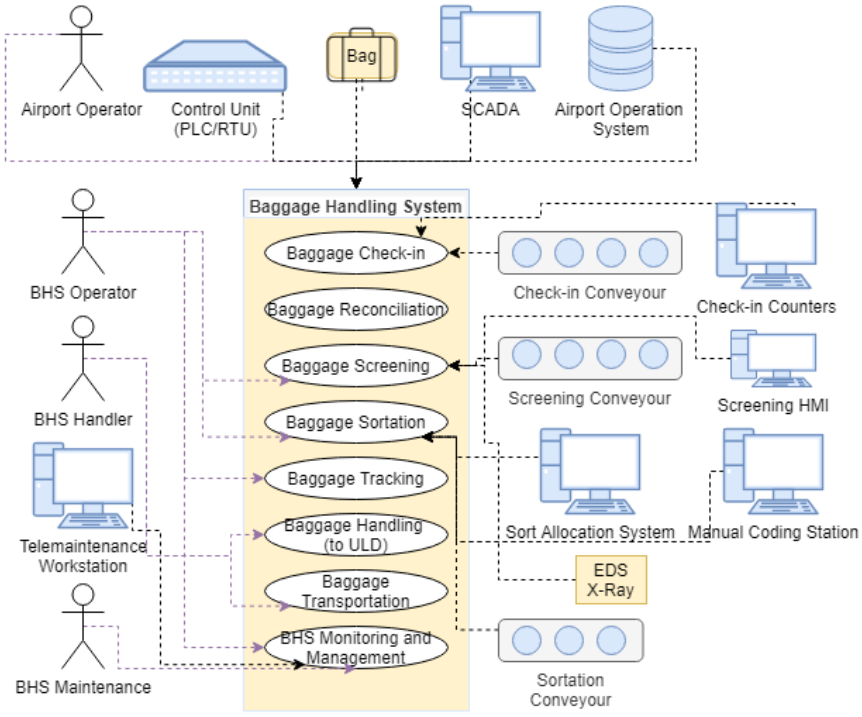

Figure 2.2: Mapping between baggage handling services and other BHS components

[4] In this case only the operation was considered until the baggage was loaded into the Unit Load Device (ULD), which is the aircraft container that carries baggage. This decision was made since BHS is only responsible for baggage that has not yet been loaded into ULD containers.

2.5 Scenario #5 – Simulation environment

This threat scenario includes cyber- and physical attacks to the air traffic management. The ultimate goal of the attacker is to intrude the frequency used for the pilot-controller voice communication, act as false ATCO to issue malicious commands, and thereby provoke multiple aircraft collisions. These two steps by themselves can easily be carried out by anyone owning an off-the-shelf Very High Frequency (VHF) radio, since the appropriate radio frequencies are publicly available. There also are multiple examples of intrusions of the pilot controller voice communication, such as 2016 at Melbourne's Tullamarine Airport (13).

However, this kind of attack is quickly detected by the real ATCOs, preventing serious consequences. The attack described in this scenario is therefore preceded by a cyber-attack on the essential air traffic management services with the aim of degrading the service for the real air traffic controllers. This causes significant disturbance and distracts them from the malicious commands issued by the attacker.

The entire attack described can be performed from the security of the attacker's home, as the flight management services are accessible from outside of the airport's network. Nevertheless, the combination with a low-risk physical intrusion into the technical cabinet room of the airport – which in some cases is directly accessible from public areas – allows the attacker to carry out a whole range of additional, even more serious attacks. Such an intrusion would also circumvent all measures that may have been implemented to prevent attacks from outside of the airport's network. Hence, a physical intrusion into the airport's technical cabinet is included in this scenario to represent the worst case, admittedly limiting the realism of the otherwise realistic attack.

2.5.1 Scenario 5 - concept

This scenario involves endangerment of ATM in addition to airport-related threats. The scenario starts with a physical intrusion into the airport's technical cabinet room. The attack continues with the compromising of a computer in order to locate essential flight management services. The attacker will then use a specific attack to gain access to this server. Having gained this access there will be a cyber-attack on the services, attempted exploitation of vulnerabilities through a manipulated Extensible Mark-up Language (XML), and other data, service and network-level attacks. This attack involves firewall intrusion, alters the switches and servers of the network, and grants access to personal data and some surveillance data. These attacks will cause a significant disturbance and additional work load to ATC controllers. In a second attack path, a false ATCO will intrude the radio frequencies used by the ATC and aircraft, issuing faked clearances to the aircraft on the ground. In combination, the two attack paths aim to create chaos in the ATC at the airport. In the end, ground movements of the aircraft may conflict, arrivals may get diverted, and there will be delays for incoming and outgoing flights. This will impact the employees on the tarmac and those in the terminal.

2.5.2 Scenario #5 - known vulnerabilities

Given that this scenario is a simulation, there are no known vulnerabilities for the simulation environment. However, the risk analysis will evaluate all possible vulnerabilities which could be present (as it will for each scenario), to determine where the greatest exposures lie.

2.5.3 Analysis of past cyber-attacks

This scenario starts with a physical intrusion into a technical cabinet of an airport, but is followed by a sequence of cyber-attacks. While a physical attack into a technical cabinet is easy enough to come up with as a possible threat scenario, the brute-force authentication and DoS cyber-attacks on flight plan services may not be. The kinds of attacks that airports should try to prevent and create management plans for include novel, innovative attacks, especially as the Information and Communications

Technology (ICT) world is constantly changing and improving. But also, the types of attacks which have happened in the past need to be considered because they present real possible threats that could happen again and indicate where advents in technology are headed, to aid in cybersecurity prevention for airports.

For example, on 2019-12-20, a cyber-attack on RavnAir occurred (14). The cyber-attack on the IT network was initially targeting the maintenance system of a specific aircraft type. The details of the cyber-attack have not been released yet, but it forced the company to shut down and knock out every part of the IT network and all company computers and servers. The immediate effect was that the company was forced to cancel eight flights on 2019-12-21. But the cyber-attack also forced them to use manual processes and back-up systems, so the company would continue to be affected for at least a month, continuing to delay flights (15).

That was not the first time that airports or aircraft companies have been targets of a cyber-attack. In March of 2018, a ransomware in the Atlanta Airport encrypted multiple official computers and forced the airport to shut off its internal Wi-Fi network as a security measure to avoid the ransomware from spreading throughout the airport network (16).

The Sodinokibi ransomware infected Albany International Airport in New York State with a supply chain attack on 2019-12-25 (17). The compromise first affected a maintenance server of the Managed Service Provider (MSP) logical net, provider of data centre services and cloud solutions, and then the attack targeted the airport's back-up servers. The airport admitted to have paid a ransom to the attackers to regain access to its data (18).

On 2019-11-04, the Spanish company MSP Everis was affected by a variant of the BitPaymer ransomware (19). Spanish local radio was also hit during the same attack campaign. The Spanish public company Aena, which manages airports and heliports in Spain, temporarily cut its networks as a preventive measure in the context of the Everis infection.

The Cleveland Airport was affected by a publicly unreported ransomware preventing the display of baggage and flight information screens on 2019-04-22. Air traffic was not impacted according to the airport authorities (20).

Nowadays airports face constant threats, and therefore it is important for airports to know about weak elements in their systems so they can take measures to mitigate the risk. This is why the SATIE scenario will involve IT and Operational Technology (OT) networks like them affected in the Sodinokibi and RavnAir attacks, the PA system like the one involved in the attack on MSP Everis and this scenario will include thoughts about attacks on FIDS like in the Cleveland Airport attack. The SATIE system will analyse available data to detect possible threats and will allow the operators to take appropriate measures in conjunction with a Security Operation Centre (SOC) to avoid threats from spreading like they did in the past.

3 Standards and Regulations

This section shows the main standards and regulations that have been taken into account for the risk assessment. In fact, a fundamental step in the risk assessment process is to carry out a gap analysis with respect to the identified security controls to highlight the presence of vulnerabilities linked to a poor or absent application of the aforementioned controls.

To cover both the cyber and physical components, security checks extracted from different families of standards have been included, following the analysis carried out with the support of end-users in D2.2, section 2.1 (12).

3.1 EU Cybersecurity Strategy & NIS Directive

The European Commission proposed a directive a European Union (EU) NIS Directive. This was a part of the EU Cybersecurity Strategy, which overall discusses how to best prevent and respond to cyber disruptions by increasing resilience, reduce crime and develop policies and resources, and establish a cyberspace policy. The EU cybersecurity strategy requires all member states to ensure that their digital environment throughout the EU is secure and trustworthy.

This NIS directive was adopted in 2016 and consists of a minimal harmonization directive, meaning its provisions are not precise. The implementation in all member states' national legislation was required by May 2018. The NIS directive specifically requires that each member state designates an authority to competently handle financial and human resources to respond to any NIS-related incidents. They must cooperate with other member states by sharing warnings on risks and incidents securely and cooperatively. Operators of critical infrastructures – including transportation – along with those in charge of information society services (e.g. cloud computing, search engines, etc.) and public administrators must all enact risk management practices and report major incidents.

A designated NIS cooperation group was created, where member states cooperate, exchange information and agree on implementation across the EU. The group is made up of representatives from various national ministries and cybersecurity agencies. In September 2017 the European Commission proposed additional cybersecurity policy initiatives, most notably a recommendation to develop a cybersecurity framework for the exchange of cybersecurity information.

In an effort to harmonize practices across the EU, ENISA published a report in 2018 prepared to offer a collection and comparison of all existing international standards on cybersecurity. The report includes the various standards and regulations which exist in the various sectors to which the NIS directive applies. In the particular application to air transport there are numerous documents taken into consideration, such as:

Standards:

1. International Civil Aviation Organization (ICAO) Aviation Security Manual - Document 8973 (Restricted Access).
2. Aeronautical Radio, Incorporated (ARINC) 811 Commercial aircraft information security concepts of operations and process framework.
3. European Organisation for Civil Aviation Equipment (EUROCAE) ED-201 – 204 Aeronautical Information System Security (AISS) Framework.
4. Radio Technical Commission for Aeronautics (RTCA) DO-326 Airworthiness security process specifications.

Best practices:

1. The American Institute of Aeronautics and Astronautics (AIAA) The Connectivity Challenge: Protecting Critical Assets in a Networked World.
2. Information Security Certification and Accreditation Handbook – Federal Aviation Administration (FAA).
3. FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access.
4. FAA Aircraft systems information security protection overview.

3.2 Privacy Regulations - GDPR

The EU implemented a General Data Protection Regulation (GDPR) on 2018-05-25 (21). This pan European data protection law extended the rights of individuals and placed new obligations on organizations with EU residents' personal data, compared to the previous data protection law (22). The GDPR aims to strengthen data protection rules by encouraging member states to allocate sufficient resources to data protection authorities, while increasing cooperation between national data protection authorities, and making full use of the tools now available so the rules are equal for all member states. The GDPR supports all involved stakeholders, ensuring that all businesses, including small- and medium-businesses can enjoy the benefits. The GDPR has 11 chapters, which include general provisions, principles, rights of the data subject, duties of data controllers or processors, transfers of personal data to third countries, supervisory authorities, cooperation among member states, remedies, liability or penalties for breach of rights, and miscellaneous final provisions. The increased rules and restrictions on data mean that people have more control over their personal data and businesses have to operate on a more even playing field. All partners, when any personal data is involved in the scope of the SATIE project, will follow all GDPR guidelines.

The GDPR requires data controllers and processors to "implement appropriate technical and organizational measures" (article 32) to protect personal data, and dedicated its Section 2 of Chapter IV to security measures (21). These measures must take into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of the processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The GDPR does not detail the security measures that should be followed. However, it does give suggestions for what types of security measures might be considered "appropriate to the risk" in article 32:

1. The pseudonymisation and encryption of personal data.
2. The ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services.
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.3 ISO/IEC 27001:2013

The International Organization for Standardization (ISO) worked with the International Electrotechnical Commission (IEC) to create an internationally-recognized best practice framework for Information Security Management Systems (ISMS). This standard aims to give specific recommendations for bringing information security under proper management control, including those related to privacy which is also contained in the GDPR and the Data Protection Act.

Security controls in organizations tend to be implemented as specific solutions to specific issues, or just as a matter of tradition. Security controls tend to address certain parts of IT, excluding non-IT aspects such as paperwork or proprietary knowledge. Or if they are included, they are often managed independently from IT. Therefore, this standard seeks to systematically evaluate an organization's information security risks, including all involved assets, possible threats, vulnerabilities, and impacts. It requires that management designs and implements a thorough plan of information security controls and other risk treatment methods to address residual risk. It also requires that management adopt a management process to ensure that the security controls actually meet the needs on a continuous basis. This standard also includes compliance with a variety of other laws such as the EU GDPR (see Section 3.2) and the NIS regulation (see Section 3.1).

3.4 ISO/IEC 27002:2013

Given that the threat scenarios in this project involve many elements of IT and that these scenarios themselves were based on cyber-physical security threats, it was imperative to include standards and best practices for information security. The ISO was created for the direct purpose of being able to create proprietary, industrial and commercial standards worldwide. Each of their standards addresses a different aspect and the ISO 27002, published in 2013 specifically addresses anything that could be managed by an ISMS (23). The standard contains ten short clauses about the standard and a long annex with all of the controls and their objectives. There are currently 114 controls contained within the 14 control categories in the following annexes:

- A.5 - Information security policies (two controls): Management direction and support for information security in line with the organization's requirements.
- A.6 - Organization of information security (seven controls): To establish a management framework to initiate and control the implementation and operation of information security.
- A.7 - Human resources security (six controls): Ensures that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
- A.8 - Asset management (ten controls): To identify information assets in scope for the management system and define appropriate protection responsibilities.
- A.9 - Access control (14 controls): To limit access to information and information processing facilities.
- A.10 - Cryptography (two controls): To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
- A.11 - Physical and environmental security (15 controls): To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
- A.12 - Operations security (14 controls): To ensure correct and secure operations of information processing facilities.
- A.13 - Communications security (seven controls): To ensure the protection of information in networks and its supporting information processing facilities.
- A.14 - System acquisition, development, and maintenance (13 controls): To ensure that information security is an integral part of information systems across the entire lifecycle.
- A.15 - Supplier relationships (five controls): To protect the organization's valuable assets which are accessible or affected by suppliers.
- A.16 - Information security incident management (seven controls): To ensure a consistent and effective approach to the lifecycle of incidents, events and weaknesses.
- A.17 - Information security aspects of business continuity management (four controls): To ensure that information security continuity shall be embedded in the organization's business continuity management systems.

- A.18 - Compliance (eight controls): To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

3.5 ICAO, REGULATION (EC) No 2300/2008

The United Nations created the ICAO in 1944 and nominated it to be in charge of the principles and techniques of international air navigation and to support the collaboration between countries to ensure safe and orderly growth of the aviation sector. The ICAO adopts standards and recommended practices for air navigation, the infrastructure, flight inspection, and border-crossing procedures. To date, ICAO members represent 192 of the 193 UN members (Liechtenstein is not included because they lack an international airport). Therefore, this is a key regulatory body for aviation standards and safety. The original ICAO Statute from 1944 has been regularly updated with additional annexes (24).

In order to cover the security measures and standards applicable within the scope of the SATIE threat scenarios, air transport specific regulations must be included and the ICAO Statute has been applied including three Annexes to ensure that the scope of the SATIE scenarios will be appropriately evaluated against the regulations to which they are subjected.

- Annex 9 – Facilitation: This Annex is about Facilitation, which involves the entry and departure of people and baggage on the planes, the entry and departure of aircraft to the airports, how passenger data is exchanged, and some other topics such as cargo which are out of scope of the SATIE project. Given that the movement and flow of passengers and their baggage is highly regulated within the airport and airplanes, these standards must be included as part of the security measures being used in the risk assessment.
- Annex 17 – Security (25): Safeguarding International Civil Aviation Against Acts of Unlawful Interference: This Annex is focused on preventing interference from unauthorized people, vehicles, or cargo and therefore focuses on checkpoints and controls, which are essential elements in the threat scenarios.
- Annex 17 update: This update from 2019 to Annex 17 focuses on detailed measures for the implementation of aviation cybersecurity. While the ISO27002:2013 standards include many aspects of cybersecurity, given that airports have specific cybersecurity standards, due to unique cyber threats they face, these standards are also included in the risk assessment.

3.6 ANSSI

The NIS Directive, discussed in Section 3.1, focuses on the security of network and information systems. However, as part of that Directive, each member state needs to transpose it into its own national laws. The National Cybersecurity Agency of France (ANSSI), is the French agency responsible for computer security. They represent France in ENISA, which is in charge of network and information security. ANSSI converted the Directive into law through 23 specific aspects, which must be adopted by all critical infrastructure sectors (including air transportation). These aspects cover the governance of the security of information systems, the protection of information systems, the defence of information systems, and their resilience. These standards were added to the security measures covered by the risk assessment to ensure proper coverage of current cybersecurity laws in airports.

3.7 Universal Security Management Systems Standard 2017

This international standard is produced by National Security Advisory Centre (NSAC) and states “the requirements for establishing, implementing, operating and continually improving a dedicated

Security Management System (SMS) for an organisation. It ensures the safety of people, and the protection of the interests and assets of the organisation against the actions of malicious adversaries such as criminals, vandals and terrorists" (26). This standard addresses the protection of all processes, people, sites, objects, infrastructures, networks, systems, tangible and intangible assets and interests of an organization and it is therefore perfectly applicable to a context such as the airport one in which there are potential criminal actions that endanger people's health, as well as the organization's business.

The standard approach is stakeholder driven and risk based following the Plan-Do-Check-Act (PDCA) cycle to continually improve the system. Moreover, it has been drafted in accordance with the high level structure for management systems of ISO. These characteristics make it easily integrated and implemented through some of the main ISO standards, such as ISO 27001 and ISO 27002.

These important points of contact further support the choice of ISO27002, integrated with some sections of regulations produced by ICAO and ANSSI, as a reference for the assessment of the application of security controls in the scenarios of the airport systems covered by this project.

3.8 Specific legal requirements of airports

There are a number of legal directives and requirements which airports must follow. The most relevant are described below.

3.8.1 Council Directive 2004/82/EC on obligation of carriers to communicate passenger data

The Council Directive 2004/82/EC establishes an obligation for airline carriers to transfer passenger data to the competent authorities according to various Articles (27). This is to improve border control and counteract illegal immigration by the transmission of passenger data by carriers to appropriate national authorities. Therefore, this ensures that the authorities on the departure side verify that the passengers are not persons of interest. Article 3 of this directive establishes that member states are responsible for enacting measures to guarantee this transmission of information on passengers moving to member state territory. The type of information that must be transmitted is also outlined, including:

- The number and type of travel document used.
- Nationality.
- Full name.
- Date of birth.
- Border crossing point of entry into Member State territory.
- Code of transport.
- Departure and arrival time of the transportation.
- Total number of passengers carried on that transport.
- The initial embarkation point.

It is also stipulated that the transmission of the above data cannot remove any obligations or responsibilities laid out in the provisions of Article 26 of the Schengen Convention, supplemented by Directive 2001/51/EC. Lastly, Article 6 sets the basis for the processing and allows for a very brief retention period aligned with the principle of storage limitation to minimize data protection issues. Member States must ensure that the data is collected by the carriers and transmitted electronically or with other appropriate means. The data shall be saved in a temporary file. After passengers have entered the Member State territory, the authorities must delete the data within 24 hours of transmission unless they are needed for later statutory purposes in accordance with Directive 95/46/EC (22). Member States must also oblige the carriers to inform the passengers in accordance

with Directive 95/46/EC. Overall, the implementation of this obligation is carried out within the EU through the Advance Passenger Information System (APIS), described below.

3.8.2 Advance Passenger Information System (APIS)

The APIS is an electronic data interchange system which allows commercial airlines, vessel operators and public administrators to exchange some passenger data elements. The elements which can be exchanged include:

- Gender.
- Date of birth.
- Nationality.
- Country of residence.
- Travel document type, number, expiration date, and country of issuance.

The guidelines outlined above indicate that Advance Passenger Information (API) must be collected by airlines and transmitted to appropriate authorities. Through the APIS, the data can arrive much sooner than would normally occur when the person reaches the immigration inspection desk. However, there are more privacy and data protection laws in many countries, such as the GDPR, and there are no guidelines about how to handle the GDPR regulations, so it must be handled on a country-by-country basis abiding by all applicable laws. In events where there is conflict, the country requiring the API should try to address and resolve those legal issues. However, within the scope of SATIE, it is already understood that the system is in operation in the European Union and complies with the GDPR so no other action or work-around needs to be executed.

3.8.3 Regulation (EC) No 300/2008

This regulation outlines the minimum security standards in civil aviation across Europe, specifically addressing common rules to protect civil aviation against acts of unlawful interference which could jeopardize the security of civil aviation (28). This regulation applies to all airports or parts of airports located in Member State territory which are not exclusively for military purposes. The Member States are responsible for ensuring that the Articles are put in place. The most relevant measures in this regulation for SATIE involve the control of restricted areas and the management of hold baggage.

Security restricted areas must be controlled to ensure no unauthorized people or vehicles enter. Each item of hold baggage must be identified as accompanied or unaccompanied. Where it is unaccompanied, it shall not be transported unless it has either been separated due to factors beyond the passenger's control or subject to appropriate security controls.

3.8.4 Discussion / Conclusion

As already outlined in the previous sections, there are many current standards and several different guidelines for standardization of safety and security procedures that apply to critical infrastructures, and more specifically to airports. As a result, a lot of security policies and tools are adopted by airports to maintain the physical and cyber security of the passengers, as well as employees. However, there are still some gaps, and these are very representative of today's challenges in cyber and physical security of the airports.

First of all, there is a lack of uniformity in the adoption and implementation of solutions that can support and enhance crisis management processes, and especially cyber protection. Among different states and airports, there is not a common adoption level and implementation of physical-cyber solutions that can support and enhance crisis management processes. Especially with regards to the cyber security the existing guidelines are broad enough, meaning that each airport decides upon their understanding for the measures to be adopted. Therefore, some airports have a very mature cyber

security posture, however, due to a several reasons, many other airports have limited capabilities or resources dedicated to cybersecurity. Moreover, even some simple best practices are not in place, for example, password reuse or sharing is common and a centralised centre for incident handling does not exist. In addition, with the introduction of GDPR and NIS directives, airports need to implement changes to ensure compliance with the new regulations and guidelines. However, as changes in infrastructures like airports, usually require the collaboration between public and private organisations, are difficult to make happen and require a lot of time. Therefore, some airports do not fully comply with NIS directives or/and GDPR law.

Furthermore, each airport is individually responsible for developing their own physical-cyber security measures. There are several guidelines and standards addressing cybersecurity practices that need to be implemented, but its interpretation and adaptation to fit an airport context is done by each airport. Therefore, standards and guidelines for the implementation of comprehensive plans for the security of airports are needed at a national level to build a common ground for all airports. It is of high value to have a series of standardized plans (risk and vulnerability assessment, security operations, crisis management, business continuity) related to preventive planning, day-to-day operation and business continuity management. Therefore, despite the importance of having security guidelines and standards that can serve as a baseline level of security processes, it is also important to ensure the consistency of its application at airports.

4 State of the art of risk analysis methodologies

The European Commission, in 2010, issued guidelines on risk assessment to assist Member States in preparing national risk assessments for disaster management. In 2014, based on the feedback provided by the Member States relevant to their risk assessments, a report produced by the Commission summarising the natural and man-made risks in the EU (29). Despite the fact that the ECI directive (30) emphasizes the importance of risk assessment for critical infrastructures at a European level, in the framework of this Directive, no risk assessment methodology was developed and Member States are following their own methodologies. Also, due to the different levels of maturity of National Risk Assessment approaches implemented by each Member State, there is no baseline for the mitigation or risk treatment methods followed. The only baseline in the risk assessment process are some intersect criteria, such as casualties, economic effects, and public effects, which are used by Member States as parameters for the impact assessment. In addition, Member State do not share common terminology, especially regarding critical infrastructure-related risk assessment (31).

Risk assessment methodologies adopted by the critical infrastructures, and more specifically airports, usually follow a standard ISO31000 approach. As such, the approach that is used is rather common and linear, consisting of some common elements namely the identification and classification of threats, the identification of vulnerabilities and the impact evaluation. This is a well-known and established approach for evaluating risk and it is the backbone of almost all risk assessment methodologies.

Risk management involves the identification, evaluation, and prioritization of risks in order to minimize, monitor, and control the probability or impact of threat scenarios. Risk management involves a plan which should be in action at all times, whereas risk assessment is done periodically to obtain a qualitative understanding of where the highest risks are within the organization and be able to accurately track changes in risk through time.

Most of the methods and tools for risk assessment originated to handle cyber environments. In-depth analyses are presented below on the tools that are most relevant in the airport environment and also take into consideration the physical aspects related to the issue of risk.

4.1 Sandia Risk Assessment Methodology

Sandia National Laboratories created and presented (on behalf of an agency of the United States government) a risk assessment methodology for the physical protection of critical infrastructures (32). It can be applied at a national level, a critical infrastructure, or anywhere in between. The proposed methodology consists of seven steps, namely: facility characterisation, critical assets definition, consequence determination, threat definition, protection system effectiveness analysis, risk estimation and system upgrades as well as impact evaluation.

4.2 National Infrastructure Protection Plan Risk Management Framework

Based on national priorities, goals, requirements for critical infrastructure, this framework supports the effective allocation of resources effectively in order to reduce vulnerability, deter threats, and minimize the consequences of attacks and other manmade and natural disasters (32). The theoretical background is a classic risk assessment framework and addresses the physical, cyber, and human considerations required, by critical infrastructure sectors for effective implementation of comprehensive programmes. The framework has six steps: goals and objectives definition; assets,

systems and networks identification; risk assessment and prioritization; to the validation of protective actions for risk reduction; as well as effectiveness measurement (33).

4.3 CARVER2

Criticality Accessibility Recoverability Vulnerability Espyability Redundancy (CARVER2) risk assessment tool was developed by NI^2 Centre for Infrastructure Expertise that is a not-for-profit, non-partisan applied research organisation, which works closely with operators, government, and the private sector in order to ensure the protection of critical infrastructures in the United States (32). CARVER2 is a tool that has been developed in order to serve the needs of critical infrastructure analysis mostly from the policy maker point of view.
The methodology incorporates six different criteria for which an asset or an infrastructure is assessed, which are the following:

- Criticality is in fact the impact assessment part of the methodology.
- Accessibility refers to the possibility that terrorists can enter the infrastructure to provoke destruction.
- Recoverability partially covers resilience since it refers to the bouncing back capability of the infrastructure after failure.
- Vulnerability covers part of the potential infrastructure vulnerabilities related to terrorist attacks, explosions and chemical/biological threat.
- Espyability is the function of an infrastructure as an icon (e.g. cultural site) with indirect impact
- Redundancy refers to the alternatives that exit for the asset in consideration.

4.4 EBIOS

Expression of Needs and Identification of Security Objectives (EBIOS) is a comprehensive set of guides and a free software product that adopts a risk management approach (34). It starts from the highest level (major missions of the studied object) to progressively focus on the business and technical elements, by studying the possible paths of an attack Figure 4.1).

It mostly addresses the needs of information system risk managers and was developed by the French government. The main aim of this methodology is the production of best practices and guidelines targeted to end-users in various contexts. EBIOS is widely used in the public as well as in the private sector, both in France and abroad, and it is compliant with major IT security standards.

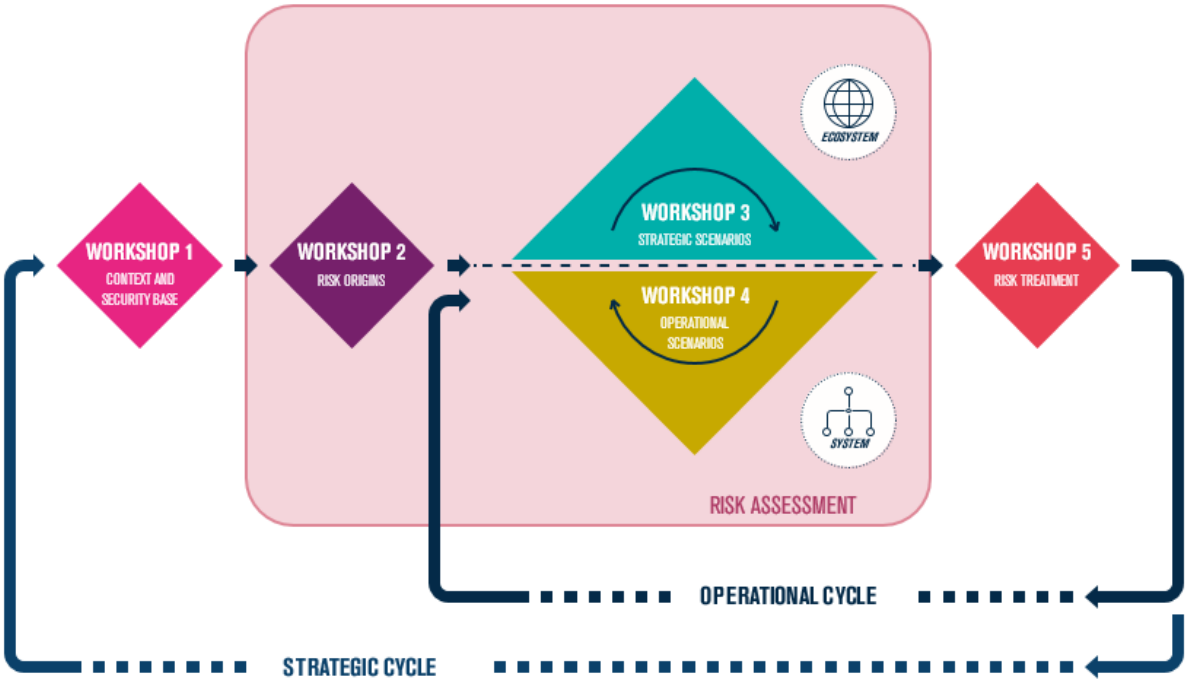

Figure 4.1: The setup of EBIOS risk manager workshops

EBIOS aims to obtain a synthesis between "compliance" and "scenarios" in order to bring the highest added value. According to the so called EBIOS risk manager, scenario-based risk assessment focuses on intentional and targeted threats. The EBIOS approach consists of a cycle of five steps as follows (Figure 4.1):

1. The first step (workshop) aims to identify the purpose of the study, the workshop participants and the time frame. During this workshop, the missions, the business values and the supporting assets related to the studied object should be identified. The threats and their impact should also be identified. The level of security and deviations from being secure should be an outcome of this step.
2. The purpose of the second step (workshop) is the identification of sources of risk and their intended objectives, in the context of the study. The sources of risk and the objectives are then characterized and evaluated in order to retain the most relevant ones. The information collected during this step will be the input for the description of the scenarios in steps three and four.
3. The scope of the third step (workshop) is the creation of a digital threat map of the ecosystem under discussion. This will allow the production of strategic scenarios (high-level). This type of scenario represents the paths of the attack in order to achieve its objective. These scenarios are evaluated in terms of severity. At the end of this step, the security measures on the ecosystem should be defined.
4. The purpose of the fourth step (workshop) is to build technical scenarios containing the operating modes likely to be used by the sources of risk to carry out the strategic scenarios. This step adopts a similar approach to that of the previous step but focuses on critical support assets.

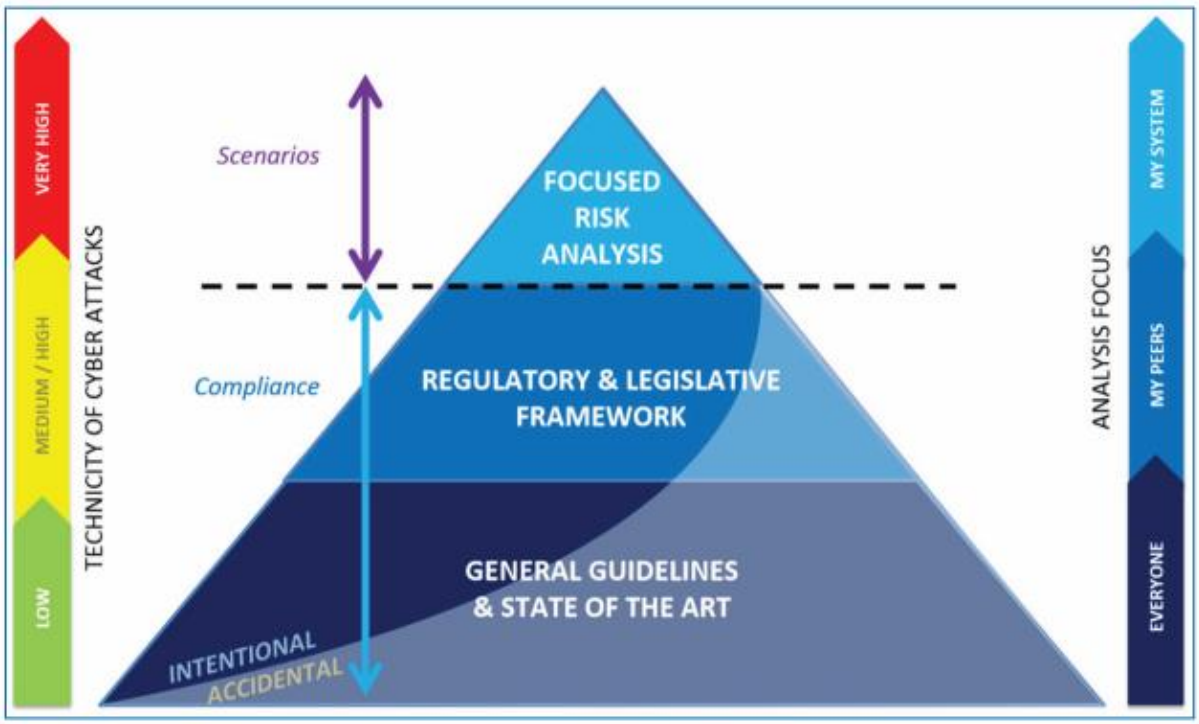

Figure 4.2: The EBIOS risk manager

The purpose of this final step (workshop) is to summarize the identified risk scenarios and define a risk-management strategy. This strategy results in the definition of security measures, included in a monitoring plan for continuous improvement of security. Residual risks are then identified as well as the framework for monitoring these risks.

4.5 SecRAM

Security Risk Assessment Methodology (SecRAM) is a risk assessment methodology created through the European Single European Sky ATM Research (SESAR) project to address security issues and consistency by the recent enactment of the Single European Sky (SES) initiative. The European Commission created SES to reform the fragmented European air traffic management system, institutionally, operationally, technologically, and through control and supervision. This initiative had the aim to increase capacity, safety, efficiency, and decrease the environmental impact of the air transportation sector. In order to meet the SES performance targets, future ATM systems need to evolve, which includes using more commercial, off-the-shelf products, incorporating open standards, and sharing more data, all of which potentially introduce new vulnerabilities. To some extent, this defeats the purpose of the SES. Therefore, SESAR developed the security management framework SecRAM, also creating awareness material, along with methods and tools to facilitate the enactment of this holistic approach to air traffic management security. While the specifics of the method are proprietary, SecRAM is seen as the foundation for the application of cost-effective, proportional and reliable security measures for the ATM system.

4.6 Bowtie

The bowtie method is a risk assessment method that can be used to analyse and communicate how high risk scenarios develop (35). The essence of the bowtie consists of plausible risk scenarios around

a certain hazard, and ways in which the organisation stops those scenarios from happening. The method takes its name from the shape of the diagram that you create, which looks like a man's bowtie. A bowtie diagram is a graphical depiction of pathways from the causes of an event or risk to its consequences in a simple qualitative cause-consequence diagram. It is a simplified combination of a fault tree that analyses the cause of an event or risk, the left hand side of the diagram, and an event tree that analyses the consequences, the right hand side. While bow tie diagrams can be constructed from fault and event trees, they are more often drawn directly from a brainstorming session, providing a fruitful basis for a group exploration of controls.

The focus of bowtie analysis is on the barriers or controls depicted to the left-hand side of the knot that can change the likelihood of the event or circumstance, or on those on the right-hand side that can change its consequences. It is used when assessing the completeness of controls, to check that each pathway from cause to event and event to consequence has effective controls, and that factors that could cause controls to fail (including management systems failures) are recognised. By combining the strengths of several safety techniques and the contribution of human and organizational factors, Bowtie diagrams facilitate workforce understanding of Hazard management and their own role in it. It is a method that can be understood by all layers of the organization due to its highly visual and intuitive nature.

In some projects, an approach whereby EBIOS is combined with bowtie is used, taking advantage of bowtie analyses of consequences and the controls that can be used to mitigate them.

4.7 OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a framework for identifying and managing information security risks (36). It defines a comprehensive evaluation method that allows an organization to identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. By putting the assets, threats, and vulnerabilities together, the organization can begin to understand what information is at risk. With this understanding, the organization can design and implement a protection strategy to reduce the overall risk exposure of its information assets.

OCTAVE is a flexible and self-directed risk assessment methodology. A small team of people from the operational (or business) units and the IT department work together to address the security needs of the organization. The team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. It can be tailored for most organizations. Unlike most other risk assessment methods, the OCTAVE approach is driven by operational risk and security practices and not technology.

4.8 SECUR-ED

The SECure URban Transportation – a European Demonstration (SECUR-ED) is an EU funded FP7 project, starting from previous work performed on FP6 COUNTERACT project, further developed, implemented and demonstrated a risk management framework for threats against urban transportation (37). The SECUR-ED risk management approach (see Figure 4.3) encompasses the typical risk management activities (e.g., ISO/IEC 31000) and aims a wide set of threats, including severe threats like CBRN, but also daily threats like vandalism, pickpocketing and other threats that public transportation operators face on a daily base.

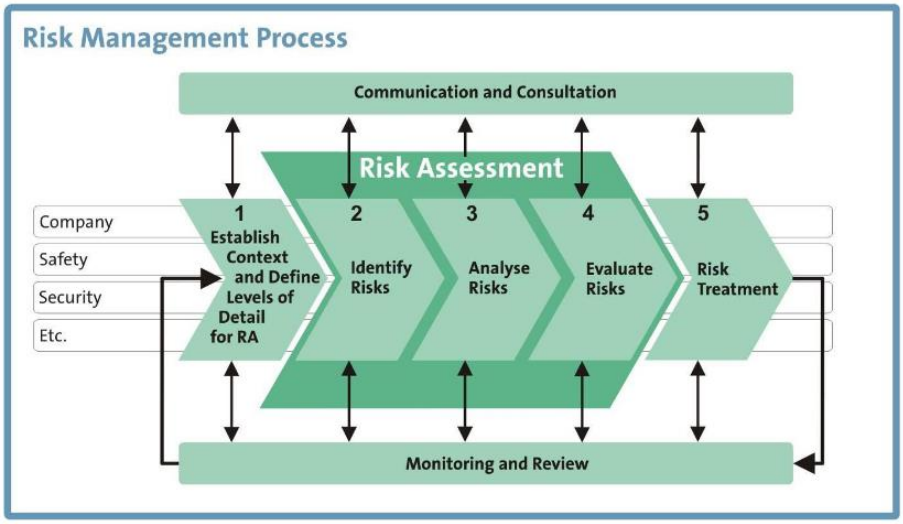

Figure 4.3: SECUR-ED risk assessment activities

The proposed approach classifies risks into different families through a multi-tier approach (e.g. on the first tier: safety, security, environmental, pandemics, etc.; on the second tier for security: business crimes, daily security threats, severe security threats, etc.) and assigning risk owners to each risk family.

Risk assessment is performed during a set of workshops with the participation of experts in the different identified risk families, although the approach is qualitative, it requires previous desk research regarding the impact and frequency of incidents in each risk families, in the organization and in similar organizations, to support the discussions.

In the risk analysis stage SECURE-ED threats against identified are assessed are according to a previously defined qualitative scale of likelihood and impact to determine the risk rank, but a additionally an evaluation of the vulnerability aspect (potentiality of a target being affected), considered in terms of weakness and/or attractiveness of the target (for perpetrators), allows the weighing of risks within each risk category allowing to include some details which usually aren't perfectly captured by impact and likelihood assessment.

4.9 RIS

The SATIE partner NIS has developed a proprietary risk assessment method, called RIS.

4.9.1 Introduction to RIS

RIS is based on the widely-used and respected management approach called PDCA, used to control and continually improve business operations. With this basis, RIS provides a systematic approach applying clear planning, implementation, and monitoring steps, able to create objective and repeatable evaluations by identifying exposed risks to business operations and to safety and security.

Risk assessment is performed on the level of the organizational operations (subsets of assets which are usually used together to complete a task) and at the level of the individual assets. The RIS method involves:

1. Defining the model (all operations, asset classes, and all the relationships with threats and vulnerabilities).
2. Determining what vulnerabilities and threats are present in the model.

3. Performing risk analysis on how those threats propagate through the organization's assets and operations and which vulnerabilities they can exploit.
4. Identifying effective risk treatment options.

The aim of the RIS method is to correctly and efficiently address changes to alleviate risks in the best way with particular regard to cyber risks but without forgetting the physical risks that can affect personal safety: while RIS was first developed to address the ISO/IEC 27001:2013 standard of information and technology security (23), it is easily adaptable to analyse a variety of standards and regulations including those related to personal security and safety. RIS calculates risk according to a function which is:

Risk = *f*(**asset criticality**, **threat impact * probability, vulnerability exposure)**

This 3-dimensional risk matrix is constructed: *criticality of the asset* ***x*** *threat levels* ***x*** *vulnerability levels*. The values of the matrix are adjustable and depend on the value scale selected, which by default is from 1-100. The numerical association with the asset criticality, vulnerability, and threat, allows for an objective risk evaluation, which is systematic and repeatable. These calculations give precise indications to stabilize security measures which should be adopted to guarantee continuation of services minimizing security risks. In a graphical view, one can visualize that applicable security measures and regulations (the grey spherical surface) protect the assets (green spheres) from threats, which can only impact the assets if there are vulnerabilities in the system (the holes in the grey surface), by missing security measures which create holes in the protection (see Figure 4.4). If the vulnerability exposure is large (diameter of the holes), the threats can potentially impact the assets more (represented as the thickness of the arrows).

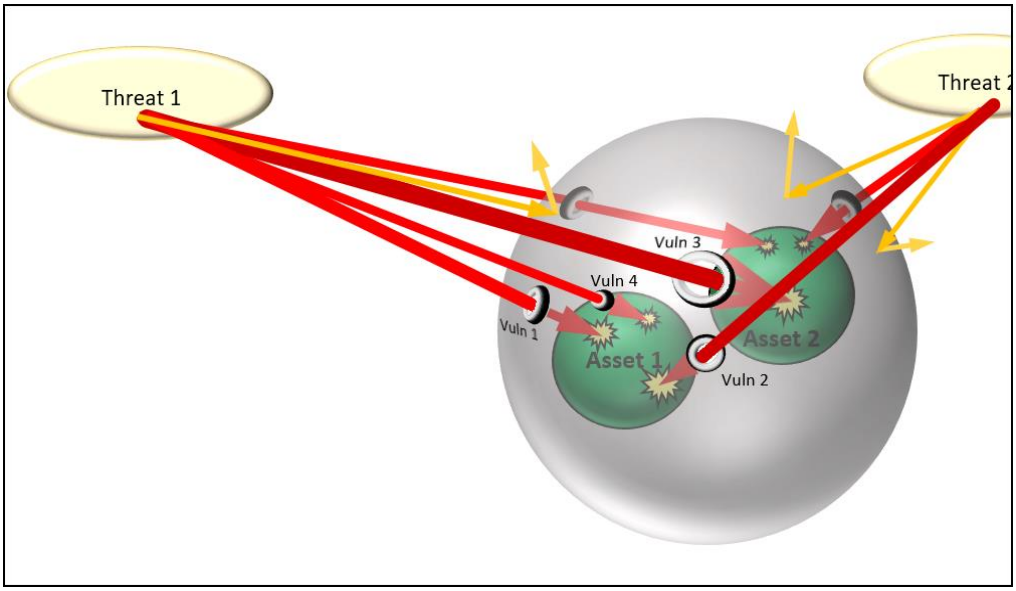

Figure 4.4: Schematic representation of how threats, vulnerabilities and assets are related

4.9.1.1 Asset criticality

The criticality of an asset affects the potential impact to the organization if that asset is attacked in some way. Therefore, through an extensive evaluation of both cyber and physical aspects, RIS allows for the systematic, comprehensive evaluation of asset criticality. RIS is made to evaluate physical assets and cyber assets, but for SATIE has been modified to properly evaluate also human assets (see section 4.11.2.1).

4.9.1.2 Threat impact

The impact of a threat is an intrinsic value, dependent on the class with which an asset has been classified and is provided in RIS libraries. The probability of a threat occurring is estimated by the

organization and is based on their physical location (to approximate threats of a natural cause) as well as their organizational structure (to approximate insider threats and operational threats). The probability only takes into account how probable someone or something is to attempt the threat, and does not represent the susceptibility or impact of that threat to the organization. This is typically a very difficult parameter to accurately estimate and it usually is based on historical information. The impact each threat can have on an asset depends on the type of asset as well as the particular attribute of the asset being evaluated (i.e. a communication infiltration threat can greatly affect the confidentiality of particular data but not the availability of it). The probability and specific impact are combined together to represent the threat's overall impact in the risk equation.

4.9.1.3 Vulnerability exposure

All assets and all organizations have threats. But the potential for that threat to be successful and impact the organization depends solely on how many vulnerabilities they have and to what degree those vulnerabilities are exposed. Therefore, RIS uses a comprehensive questionnaire based on the chosen security measures to evaluate how well the organization protects itself from vulnerability exposure. The analysed security measures are taken from the main international standards and regulations, as well as from sector specific set of controls. This approach leads, as a first result, to a gap analysis that can show how the identified security measures are currently applied at the organization's sites. This preliminary result is used as an input to evaluate the level of exposure of the assets to the vulnerabilities: if security measures are not in place (e.g. requiring passwords to enter applications, requiring confidentiality clauses in contracts, etc.), then there are significant gaps in the protection of the organization and assets (see section 4.11.1.3) with respect to some specific threats related to the abovementioned vulnerabilities. RIS is adaptable to include any security measures applicable to the organization, and calculates vulnerabilities as a measure of how well those measures are enforced. The greater and wider the number of security controls and standards introduced in the process is, the more exhaustive is the analysis of vulnerabilities present in the organization, allowing to cover both cyber and physical aspects. For this reason, the gap analysis can be seen as a part of the risk analysis process, able to identify the vulnerabilities, one of the three components of the risk.

4.9.1.4 Risk

Ultimately, the risk comes from how impactful and probable a threat is, how critical an affected asset is, and how open or exposed the organization is to particular vulnerabilities. The risk can be evaluated per asset. A risky asset indicates not only that it is a critical asset, but it is also highly exposed to vulnerabilities associated with a probable, impacting, threat. The risk can also be evaluated per threat, which means the threat is associated to that risk, and could be high due to the association of critical assets or highly exposed vulnerabilities to that threat, or a combination of the two. At the same time, risk can also be evaluated per vulnerability. This indicates that the vulnerability is associated with a high risk, and often has a high exposure level or is associated with multiple critical assets. Countermeasures to address the risk should take into account all aspects of the risk: asset criticality, the impact and probability of threats and exposure to vulnerabilities. Ultimately the organization cannot change the probability of a threat occurring, nor the criticality of an asset, but by improving how well security measures are enforced in the organization, they can reduce their exposure to vulnerabilities, which allow said threats to impact the assets.

The RIS method includes risk analysis, risk identification, and risk treatment. After the risk analysis is performed, the resulting risk value is compared to the risk appetite to reveal what residual undesirable risk remains above that threshold which should be addressed. This, therefore, is the risk identification. To treat the risk, countermeasures can be selected based on their ability to mitigate risk, while taking into account cost, efficiency, and a lack of alternatives.

4.9.2 Specifics of the RIS methodology

4.9.2.1 Evaluating asset criticality

To determine how critical an asset is, RIS uses specific attributes by which to measure the criticality. Risk assessment is performed by businesses worldwide to determine the greatest risks to their assets and/or operations (depending on the objectives of the risk assessment). But understanding weak points in the system is only useful if there are goals in mind. In other words, why does it matter if a back-up server breaks or if sensitive data were accidentally publicized? Risk analysis is performed with the goal of determining how that would impact particular business attributes such as the company's public reputation, financial impacts, or their ability to follow legal cybersecurity regulations. RIS allows for a selection of multiple business and safety attributes (up to 10) to include in the evaluation (the categories of included business attributes are found in). They can also be weighted unevenly, if, for example, safety and security to human life should count more than financial impacts. Through this selection and weighting of attributes according to the organization's priorities, the risk results subsequently reflect that prioritization.

4.9.2.2 Determining threat probability

This step is vital and includes all possible threats which may impact the assets. Based on the asset types included in the project, all possible threats are automatically included, together with their potential impact value. To help interpret the results later on, the threats are grouped according to type: environmental causes (e.g. flooding, blackout), natural causes (e.g. bad weather conditions, earthquake), technical causes (e.g. communication equipment failure, network overload), behavioural or situational accidents (e.g. personnel tiredness/stress, maintenance error), voluntary behaviour (e.g. theft, listening to unauthorized communications), and terrorism or sabotage (e.g. false information insertion, bomb). Informed personnel give a qualitative probability of each threat at the level of the organization. At this stage, this does not represent the likelihood of them negatively impacting the organization, but rather how present that threat could be in the environment of the organization. While these are determined at applied to the organization as a whole, when each asset is added to the inventory, its applicable threats are automatically loaded with the corresponding probabilities, but these can be adjusted specifically for that asset. This allows for an even greater personalization and precision in representing the probabilities of threats to each asset.

4.9.2.3 Evaluating vulnerability exposure

In order to determine vulnerability exposure, there must be some standards or set of security controls with which to calibrate. The step of vulnerabilities identification is critical for the assessment of which specific risks are present. The identification of all possible vulnerabilities is automatic in RIS, based on the previously included threats (which again, are based strictly on the types of assets present). However, the levels of exposure to these vulnerabilities are determined through checklists of questions which are submitted to the operation managers. These questions were created to address the safety and security controls associated with this project so that every aspect of the possible vulnerabilities can be assessed. Once all the questions are answered, by knowledgeable personnel about the procedures and situation in the organization, every vulnerability will have one value to represent its overall exposure of a particular threat to a particular asset. Vulnerabilities can be grouped according to seven categories: personnel security, environment and physical security, computer and network management, control of access, operational management, conformity management, and administrative management. Threats almost always are associated with more than one vulnerability; therefore, every threat-vulnerability relationship can be assigned a qualitative value of *very-low*, *low, medium, high* or very-*high.*

4.9.2.4 Risk assessment results

This chain of relationships that links asset classes, threats, vulnerabilities and security controls is the backbone of the RIS methodology. Using the values of each of these elements, the calculation for risk assessment can be applied.

There is always some degree of risk present by the fact that there are assets and people interacting with assets. However, it is important to identify what baseline level of risk is acceptable which the organization can tolerate in order to identify which risks, above that threshold, must be addressed. A common practice is to perform a preliminary risk assessment on one particular system within the organization which is well-understood and whose risks are considered acceptable. Then, based on the level of risk that system has, the organization can decide that is the threshold above which the risks should be addressed in some way.

The results of the risk assessment can be visualized from various points of view. There is a view of the risks associated with the asset, arising from the various threats that may loom over it and from the vulnerabilities to which it may be exposed when such threats occur. It is also possible to analyse each threat, which shows which vulnerabilities can be exploited and the assets with high risk values for that threat. Similarly, other aggregations of data are performed on the level of operations, systems, etc.

With the risk results and the identified risk appetite, the risks which need addressing can be identified. In this case, appropriate countermeasures must be put into place to bring the level of risk down to an acceptable level. Each asset is assigned to a Risk Manager, in charge of deciding on appropriate countermeasures to implement, among the four main standard options for risk treatments:

- Risk mitigation – the application of appropriate control measures.
- Risk (conscious) acceptance - verifying that all policies are still being satisfied.
- Risk avoidance - meaning the elimination of risk by re-engineering the processes, avoiding the processing of certain information, or particular technological solutions (if possible).
- Risk Transfer – this is based on stipulations in the insurance policy or through outsourcing.

The risk management processes can be driven by RIS through simulation with “what-if scenarios” of how the risk values would decrease based on particular changes in the enforcement of the security measures selected.

4.9.3 Advantages

Risk analysis is an essential element in the critical infrastructure world. Operations must be protected against threats, especially those related to personal safety. Organizations, including those involved in the SATIE project, generally seek to aim their efforts, temporal and economic, towards abating the most probable and dangerous risks. RIS aims at providing a big-picture view of the situation, making results easily and quickly attainable, and at the same time there are ways to quantify the risk and determine which assets or operations are at risk and by how much, allowing for better prioritization of countermeasure efforts, and allowing for precise changes to be tracked over time.

RIS utilizes both qualitative (determining if a probability is low, medium, or high) and quantitative approaches (numeric values calculated based on the negative safety and economic impact if particular vulnerabilities to an asset were to be exploited). Taking advantage of both approaches, the risk assessment offers both numeric values to risks - precisely indicating where the organization should put their security efforts and precisely predicting how that will mitigate their risk - while also granting an intuitive, big-picture overview of which operations are more at risk without requiring expert knowledge.

This dual approach allows for a more intuitive evaluation (qualitative) while outputting numbers so that unbiased calculations and comparisons can be performed. RIS offers a quantitative way to identify the weakest points in the organization – at the asset level or operation level – and to compare possible countermeasures to best reduce the residual risk. RIS is a complete risk assessment methodology, ideal for personal-, physical-, and cybersecurity assessment.

4.10 Comparison of risk assessment solutions

When deciding which risk assessment solution to use, some of the most common, commercially-available solutions were excluded because this project requires much more flexibility. This flexibility is necessary both in the regulations and security controls being covered in the assessment because of the uniqueness of the air transport sector, and also flexibility is necessary in the ability to implement the solution on the SATIE platform and integrate it with other modules. Therefore, more customization and flexibility is necessary than an off-the-shelf solution can offer. Below is a table comparing the previously discussed solutions (see section 4) regarding the most vital aspects relevant to this project.

As this project focused on cyber-physical threat scenarios, it was imperative to choose a risk assessment methodology which could include both cyber and physical assets, as well as human assets, in order to fully cover aspects of human safety and security. Strictly related, it also was imperative that the solution was adaptable to different standards and regulations. The selection was done since the proposal, after a preliminary scouting and analysis of the state of the art. A more in-depth analysis was carried out during this task and confirmed the main elements supporting the original choice of RIS.

Some of the best candidates to play the role of a risk assessment framework and solution in the context of SATIE are EBIOS and SECRAM. However, there are some important limitations to the adoption of such solutions. EBIOS, as discussed above in Section 4.4, is a risk assessment method developed in France but commonly used in many countries and applied to various sectors. It has had much success, but it is limited to analysing digital risks, which was the purpose of its creation. Therefore, an approach which also includes physical risks is essential for the proper analysis of this project's five cyber-physical threat scenarios. On the other hand, SecRAM, as discussed in Section 4.5, was developed specifically for the air transport sector and in particular, national ATM to harmonize and quantitatively evaluate the risks in that unique field. It also includes the management of physical assets and represents one of the methodologies that are closest to the needs of the project. At the same time, the methodology adopted in RIS has many aspects in common with SecRAM and, being a solution developed by a partner of SATIE, it guarantees an adaptability to the project objectives and a flexibility that is difficult to find in other market solutions.

RIS was originally created for IT environments but it was enhanced for this project and it uses libraries with the main physical assets, threats and vulnerabilities. Moreover, this tool is particularly adept at being able to incorporate new and sector specific physical assets, as well as threats and vulnerabilities, because of how it works (based on the application of both standard and custom security measures and regulations): these elements have been further integrated with those characteristic of the SATIE scenarios to offer full coverage. RIS is not only able to accommodate both physical and digital assets, threats, vulnerabilities, and add on other regulations, but it also offers more points of view in the type of results it gives: the risk results can be expressed at the level of assets themselves, of threats, and at the level of operations, which is very useful from an operational point-of-view of an airport, which is a complicated system-of-system. Therefore, the RIS tool was chosen as the optimal solution.

Finally, no less important for the adoption of RIS, was that using a tool which one of the partners of the project has in-house meant that there was much more flexibility: the possibility of modifications to create a solution suitable for the purposes of the project and integrated with other modules of the platform (i.e. the asset repository managed through Gestionnaire Libre de Parc Informatique [GLPI], the vulnerabilities via Vulnerability Intelligence Platform [VIP]).

Table 4.1: Comparison of risk assessment tools

Aspect	Sandia	NIPPR	CARVER2	EBIOS	SecRAM	Bowtie	OCTAVE	SECUR-ED	RIS
Applicable sectors:	National Level / CI	CI	CI (US)	IT	Air Transport	Aviation and high risk scenarios	IT	Public transportation	IT/Others
Includes physical assets?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Includes digital assets?	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Covered regulations:	N.A.	N.A.	N.A.	ISO 15408, ISO/IEC 27005, ISO/IEC 27001, ISO 31000.	ISO/IEC 27002, NIST SP800-53, ICAO.	Custom controls	N.A.	ISO/IEC 31000	ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 20000, ISO 31000, others are configurable.
Risk results in terms of assets?	No	Yes	Yes	No	Yes	No	Partial	No	Yes
Risk results in terms of threats?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Risk results in terms of operations?	No	No	No	No	No	No	No	No	Yes
Results include countermeasures?	No	Partial	No	No	Yes	Partial	Partial	No	Partial
Approach	Basic RAM framework adapted to meet requirements of different CI sectors	Coordinated approach to establish national priorities, goals, and requireme	Cross-sectoral approach. Useful for Homeland Security-related	Self-assessment and discussions in a mixed work group	Holistic approach to air traffic management security: foundation for the application	Analysis and demonstration of causal relationships in	Self-directed approach, driven by operational risk and security practices:	It encompasses the typical risk management activities and aims a	Holistic and flexible approach to risk, with respect to different sectors and systems and

		nts for CI and key resources protection	assessments	(managers, IT and users)	of cost-effective, proportional and reliable security measures for the ATM system	high risk scenarios	people from an organization assume responsibility for setting the organization's security strategy	wide set of threats, including severe threats and daily threats	with respect to different families of security controls
Complexity	Medium	Medium	Medium	Medium	High	Low	Medium	High	High

From a security perspective, this project deals with highly sensitive and critical information for airport operations, and thus, for security reasons some information needed to be anonymised. On top of that, needing to handle EU-restricted information for this risk assessment meant that also the risk assessment tool needed to abide by EU-restricted security constraints, which required installation and use on an air-gapped computer (along with other measures). Therefore, having the tool in-house meant that this kind of management of the tool and the contained information as well as reports and outputs could be customized and changed as needed. Also any system communication and integration messages sent to other modules on the SATIE platform could be modified as necessary, which no other off-the-shelf risk assessment tool can offer.

Regarding the topic of sensitive and personal data, throughout this task ERI worked with the partners to evaluate what data would be handled and concluded that this task does not involve any personal data, nor do the assets included in the risk assessment contain personal data. Therefore, it was not necessary to select a solution which covers GDPR for the purpose of this risk assessment activity.

The security issues are also strongly related to the opportunity of comparing the risk assessment results collected with RIS with other state-of-art risk assessment methodologies and solutions already in use at airports. While it would not be feasible security-wise to gain access to airport in-house risk assessment methods and results, a solution was decided upon to obtain a meaningful comparison that leverages the validation activities, within the framework of WP6. To compare the results from RIS with the in-house risk analysis results, the end-user specialists will be directly involved and they will follow necessary regulations and thus avoid their sensitive methods and data to leave airport borders. In this way, the airports' sensitive information stays in the airports' own hands, still producing a valuable and qualitative comparison.

4.11 RIS into the SATIE world

One of the main reasons why RIS was chosen as the risk assessment method for SATIE, as mentioned in section 4.10, was due to its adaptability. It is uniquely able to be personalized without significant changes to its configuration.

In order to achieve such personalization, there was close collaboration between NIS, the technical partners and the end-users. On top of that, there were three scheduled in-person meetings with all involved partners, each one hosted by an airport end-user. During the course of these focus group meetings, time was designated to discuss and gather necessary information to make significant progress on the tasks of the work package. These in-person meetings were followed by regular meetings and e-mail exchanges to gather the necessary information. Along with discussions for the deliverable D2.2 about the current standards and guidelines in place which must be considered within the context of SATIE (12), three essential standards were identified thanks to the airport end-users. These standards were discussed in section 3, in addition to how the rest of the necessary information was decided on and collected for the risk assessment.

4.11.1 Tailoring the RIS methodology for SATIE

Although the whole methodology was only partially re-engineered for SATIE, all elements of the risk assessment were personalized for SATIE. The following sections describe those personalizations or tailoring.

4.11.1.1 Asset inventory

The asset inventory of RIS is normally personalized for the organization – although there is the possibility to use a default IT-focused asset inventory – and therefore much time and discussion was spent on the asset inventory to ensure full coverage of all assets within the scope of the scenario and

sub-dividing the human assets into as many different categories as possible. For example, not only airport employees were included as would be expected, but they were sub-divided into employees with differing levels of clearance or whether they physically are land-side or air-side, depending on which designations made the most sense for the scenario. In doing this kind of specific analysis and making these distinctions, better risk analysis could be performed based on what security measures they are subjected to and thus which threats can affect them. The asset inventory was tailored as much as possible for the context, while the tailoring done for the other three inputs to the risk assessment is what really make the RIS tool uniquely suitable for the project.

4.11.1.2 Cyber and physical airport specific threats

Many new threats were created and added to the risk assessment to better address the potential physical damage to humans (e.g. compromised personnel, bomb, pandemic, etc.) and to include unique airport-specific threats (e.g. melee attack, vehicle-ramming attack, insider threats which can impact critical airport systems, etc.). The compromised personnel threat was also divided into three levels to differentiate the potential impacts of a compromised personnel with no security clearance, those with medium security clearance and those with high security clearance. The latter could impact many more types of assets, but the probability on average is lower. Even further, each of those threats was divided into a cyber-related threat and physical-related threat because a compromised person with a particular level of clearance can threaten assets differently depending on whether they are physically threatening them or performing cyber threats. As discussed in much more detail in D6.2 section 2.1.1 (2), there have many attacks and instances of compromised personnel at airports performing illegal or dangerous activities, and thus it was crucial to include this threat and better distinguish between the various types of personnel.

4.11.1.3 Included security measures

The RIS risk assessment was originally developed, as described in Section 4.9.1 to address the ISO/IEC 27002:2013 standards and to address risk from a IT governance perspective. The reason behind this choice is that if particular security measures and best practices are not in place or poorly applied, assets are vulnerable to potential threats. Therefore, by using a set of standards and best practices, RIS can determine the amount of vulnerabilities and consequent risk to assets and to operations based on how well those security measures are in place. To that end, the end-users decided that the following three standards and regulations should be included in order to cover all pertinent cyber and physical aspects within the scope of the scenarios:

1. ISO27002:2013 – which is the international standard for information technology.
2. ICAO Statute – which covers international air transport specific regulations applicable to all UN member states.
3. ANSSI.

This is an important benefit of the RIS method: because it measures vulnerabilities through compliance to applicable regulations and security measures, it can easily be adapted to include any type of regulation. Similarly, having RIS in-house as proprietary software of one of the partners in SATIE, the end-users could select the regulations most necessary and NIS modify the risk assessment accordingly. Questions were created based on these standards and each question, within RIS, was linked to one or more security controls of these standards: in this way any resulting high risk could be traced back to the control(s) which should be applied better to ameliorate the risks. The areas that these three standards cover were described above in section 3.

With these modifications made to RIS, vulnerabilities could be accurately assessed which relate to the proper screening through security by third-party vendors or the continuous surveillance of passengers or the use of whether background checks are mandatory before issuing airport employee IDs, to name some examples. These types of physical and insider threat vulnerabilities were added in addition to the IT-related vulnerabilities, which are similarly crucial for critical airport systems.

4.11.2 Innovations to the RIS methodology for SATIE

Beyond the elements which were tailored, some underwent innovative, configurational changes. As discussed in section 4.9.1, RIS requires that an asset inventory is created, threat probabilities are determined, compliance to security measures are recorded, which then determine vulnerability exposure. All those aspects were tailored for the SATIE project. However, to better suit the needs of the project and create an innovative methodology to manage combined cyber and physical aspects in the risk assessment of an airport organization, two particular aspects were designed and implemented. In the following sections an overview of them is presented.

4.11.2.1 Asset inventory and criticality evaluation

During the creation of the asset inventory, each asset is evaluated in a systematic way to determine its criticality. The standard procedure was described in section 4.9.2.1, but the innovative aspect for SATIE was that an additional attribute was added, called '*Safety & security of people*'. This attribute includes both intentional and unintentional possibilities: while threats can be specifically identified as a part of safety or security, regarding the overall impact on other people, both properties are included here. In this way, when each asset is being evaluated, its effects are not only measured against how negatively that would impact operational, business, reputational and compliance aspects of the organization, but also against how that would impact the *Safety & security of people*.

Moreover, any attribute is evaluated by its "standard" CIA (confidentiality, integrity and availability) parameters and by a new *safety & security* parameter. Just like the other business attributes, safety & security is expressed as a value representing the potential negative impact on the safety & security of people – passengers, personnel, third-party staff, etc. – if the asset were negatively impacted.

This leads to a better and holistic evaluation of the important aspects of the asset: during the evaluation of an asset, the impact to the business attributes and *Safety of people* were evaluated based on if the asset's confidentiality were lost, if its integrity were lost, if its availability were lost, and if its own *Safety & security* were lost. In the evaluation of a non-human asset, this last category was obviously excluded (see Table 4.3). But for human assets, such as a police officer, it could be evaluated based on what kind of impacts there would be if the police officer's own *Safety & security* were lost, how that would affect business relations, but also how that would impact the Safety of people in general. If a police officer were harmed or injured, that would logically have a larger negative impact on the Safety of people than if a third-party duty-free employee were injured. This ultimately allows for the risk analysis to reflect the risks to *Safety of people*.

Table 4.2: How attribute categories (rows) should be analysed for each asset qualitatively (columns)

Attribute	1 - Very low	2 - Low	3 - Medium	4 - High	5 - Very high
Safety & Security of people	No injuries.	Minor injuries.	Severe injuries.	Multiple severe injuries.	Fatalities.
Operational	No change in quality.	Minor inability to manage resources.	Inability to manage resources, which makes a system partially inoperable.	Major Inability to manage resources, which makes a major system inoperable.	Major inability to manage resources, which makes multiple major systems inoperable.
Business	No effect.	Minor loss of income.	Large loss of income.	Serious loss of income.	Bankruptcy or loss of all income.
Compliance	No impact.	Minor regulatory infraction.	Multiple minor regulatory infractions.	Major regulatory infraction.	Multiple major regulatory infractions.

Attribute	1 - Very low	2 - Low	3 - Medium	4 - High	5 - Very high
Reputational	No impact.	Minor complaints.	Complaints and local attention.	National attention.	Government & international attention.

To summarize, the achievement of a more detailed and effective assessment is targeted through the evaluation of negative impact on the business attributes in four distinct ways, with a numeric value for each one:

- **Safety & Security**: This assesses the potential negative impact on the organization if the asset's safety or security were lost. For human-related assets, if their safety or security were lost, this would have significant repercussions for business objectives, reputational attributes, as well as impact the safety and security of other humans (e.g. *How impactful would it be to the organization's operations if the police were physically hurt or injured?)*. Again, this includes physical harm due to either intentional or unintentional causes.
- **Confidentiality**: This evaluates the potential negative impact on the organization if the confidentiality of the asset were lost, whether intentionally or unintentionally, possibly resulting in unauthorized individuals having that information (e.g. *How impactful would it be to the organization's operations if the data on this database were no longer confidential?)*.
- **Integrity**: This is expressed as a value representing the potential negative impact on the organization if the integrity of the asset were altered; whether accidental or intentional (e.g. *how impactful would it be to the organization's operations if the integrity of this data on the database were lost and no longer reliable?)*.
- **Availability**: This is expressed as a value representing the potential negative impact on the organization if the availability of that asset were lost, accidentally or deliberately (e.g. *how impactful would it be to the organization's operations if the data on this database were no longer available?)*.

Not all of these aspects are applicable to every asset type. Therefore, the aspects marked with an X are evaluated for the assets according to Table 4.3.

Table 4.3: Applicable asset aspects to evaluate for asset criticality

	Safety & Security	Confidentiality	Integrity	Availability
Cyber assets	N.A.	X	X	X
Non-human physical assets	N.A.	N.A.	X	X
Human assets	X	N.A.	N.A.	X

The loss of these four independent aspects of the asset and how that would impact the ten potential business and safety attributes allows for the complete and comprehensive determination of the asset's criticality.

Category	Attribute	CONF	INTEGR	AVAIL	SECURTY-SAFE...
FINANCIAL IMPACT (Compliance)	Disattended Regulatory/Legal obligations	N.A.	N.A.	N.A.	N.A.
CUSTOMER IMPACT (Business)	Delayed release or unability to deliver SLA	N.A.	N.A.	N.A.	N.A.
CUSTOMER IMPACT (Reputational)	Customer dissatisfaction and loss of existing/prospective customers	N.A.	N.A.	N.A.	N.A.
CUSTOMER IMPACT (Compliance)	Disattended Contractual obligations	N.A.	N.A.	N.A.	N.A.
FINANCIAL IMPACT (Business)	Revenue reduction/Additional costs	N.A.	N.A.	N.A.	N.A.
FINANCIAL IMPACT (Reputational)	Negative public perception	N.A.	N.A.	N.A.	N.A.
INTERNAL IMPACT (Business)	Inability to achieve business targets	N.A.	N.A.	N.A.	N.A.
INTERNAL IMPACT (Operational)	Inability to manage resources, change and capacity programmes	N.A.	N.A.	N.A.	N.A.
INTERNAL IMPACT (Compliance)	Disattended Internal Policies requirements	N.A.	N.A.	N.A.	N.A.
SAFETY	Personal impact (Safety)	N.A.	N.A.	N.A.	N.A.

Figure 4.5: The matrix to fill out to determine the criticality of an asset in RIS

These components from which the assessment of the criticality of the assets derives will then be kept separate during the course of the entire analysis in order to obtain an overall risk assessment but also at the level of each of them: not only the risk that insists on an AODB, but also the importance of its components of confidentiality, integrity, availability and safety & security (where applicable).

4.11.2.2 Integration with propagation model

In an airport environment, as well as for any critical infrastructure, it is particularly important to not only understand risks to critical assets, but how that risk of threats propagates through connected assets or systems. When one system is attacked, there is a high likelihood that other applications or systems will be impacted. Attackers increasingly use combined attacks that start from a more easily accessible system to achieve more ambitious targets on critical systems, moving within the asset network (made by cyber and physical elements) of the airport infrastructure.

Therefore, a novel reconfiguration of the risk analysis was to include a risk propagation model. The risk results from RIS will be integrated with FHG's threat propagation model (defined in T2.4 and implemented in T5.1) to show how the risk values propagate through chains of assets based on their interrelations and potential threat propagations (e.g. a cyber-threat of *technological equipment tampering* can transform into a physical threat of *unauthorized access to physical areas* if information related to access control is impacted). In this way, the risk results can provide the organization with useful information about how to break these "chains of risk" and properly manage system-of-systems which are highly interconnected.

5 Conclusion

The current deliverable is focused on the definition of background scenarios on cyber-physical threats and vulnerabilities that are typical of attacks which threaten airport infrastructures. While considering each of the three different airport sites and analysing their peculiarities and potential exposures to cyber and physical attacks, a representation of the scenarios was created. This includes all elements relevant to perform an assessment and a risk analysis of the airport assets and operations in scope. The methodology defined and implemented is ISO31000 compliant and includes security controls from the most relevant standards identified in task T2.1 of the SATIE project: ISO/IEC 27002:2013, ICAO (annexes 9 and 17-18), and ANSSI best practices.

An important harmonisation was done with respect to the airport operations identified and for each end-user's scenario. This allowed obtaining a set of results with a common baseline. Each scenario is now represented by common elements like operations, assets, vulnerabilities, security controls and more attributes that can be used in the task T2.4 to design the impact propagation and decision support model. At the same time, these scenarios are the background for subsequent project activities which have the aim of designing and implementing the SATIE Solution based on this information.

Based on the threat scenarios, methods and techniques have been implemented and integrated to respond to specific airport security requirements. This allowed for the providing of a solution to perform an assessment in a tailored scope of the airport operations. The RIS tool will be further integrated with the overall platform to provide an assessment to the preparedness phase of the crisis, based on a common set of data with the other modules of SATIE. In T3.1 we are proceeding to integrate with the GLPI asset repository in order to have a common basis to represent the attack scenarios and analyse them. The RIS interface will therefore be available to operators to analyse the risks detected periodically and implement treatment plans aimed at mitigating them. Moreover, an integration with the propagation model (T2.5) will allow RIS to show a more exhaustive representation of the risks, linked to the interactions between cyber and physical threats, that can represent complex attack scenarios.

A close collaboration was constantly maintained with the end-users, throughout the definition of the scenarios, the collection of the inputs, and the presentation of the results. During the latter, for example, an attempt was made to compare the results that emerged from the activities previously carried out by end-users, as well as from their precepts, with those that arose from the results of the complete risk analysis on the five scenarios. Stakeholders were important players in this analysis process, contributing with their experience both in the design of the scenarios and in the collection of information in order to carry out the risk assessment.

This risk analysis carried out in parallel on the five scenarios, according to ISO31000 guidelines, has allowed for the highlighting of both common elements between the various airports in the management of cyber and physical security issues, and significantly diverging elements. It is clear that there is a different perception of the existing security measures, translated, for example, into critical levels assigned to similar assets in a very variable and diverse way between one end-user and another.

The results achieved cannot and in no way aim to be exhaustive, but they nevertheless represent the foundations on which the following WPs of the project can base their own designs and developments.

6 References

1. **European Commission.** Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Euorpe. [Online] [Riportato: 16 November 2020.] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-infra01-2018-2019-2020.

2. **SATIE project.** *D6.2 Test, validation and demonstration scenarios.* 2020.

3. **Metrojet Flight 9268. *Wikipedia.* [Online] [Riportato: 10 November 2020.] https://en.wikipedia.org/wiki/Metrojet_Flight_9268.**

4. Stuxnet. *Wikipedia.* [Online] 17 November 2020. [Riportato: 19 November 2020.]

5. Ruby, C. L. The definition of terrorism. *Analysis of social issues and public policy.* 2002, Vol. 2, 1, p. 9-14.

6. Johnston, Barry R. e Nedelescu, O. M. The impact of terrorism on financial markets. *Journal of Financial Crime.* 2006, Vol. 13, 1, p. 7-25.

7. Araña, J. E. e León, C. J. The impact of terrorism on tourism demand. *Annals of Tourism Research.* 2008, Vol. 35, 2, p. 299-315.

8. IBM. *Reviewing a year of serious data breaches, major attacks and new vulnerabilities.* 2015.

9. IATA. *IATA.* [Online] 2019. https://www.iata.org/contentassets/a7065984fea6447fa3b738c844c97ebb/iata-blue-skies-white-paper-2019.pdf.

10. ENISA. *ENISA Threat Landscape 2020 - Insider Threat.* s.l. : ENISA, 2020.

11. Oxford Circus panic. *Wikipedia.* [Online] 19 September 2020. [Riportato: 11 November 2020.] https://en.wikipedia.org/wiki/Oxford_Circus_panic.

12. SATIE project. *D2.2 - SoA about airports security and expected improvements.* 2019.

13. Johnston, Chris and Carmody, Broede. Lone-Wolf Radio Hoaxer Hacks Melbourne Air Traffic. *The Age.* [Online] 7 November 2016. https://www.theage.com.au/national/victoria/lonewolf-radio-hoaxer-hacks-melbourne-air-traffic-control-afp-20161107-gsk12o.html.

14. Ravn Group. Ravn News. [Online] 30 December 2019. https://www.flyravn.com/category/ravn-news/.

15. Kirby, Daniel. Cyber attack on RavnAir forces cancellation of Alaska Dash 8 service. [Online] 21 December 2019. https://www.ktuu.com/content/news/Cyber-attack-on-RavnAir-forces-cancellation-of-Alaska-Dash-8-flight-service-566406781.html.

16. McMillan, Robert. Atlanta Hit with Cyberattack. *Wall Street Journal.* [Online] 23 March 2018. https://www.wsj.com/articles/atlanta-hit-with-cyberattack-1521823062.

17. Gatlan, Sergiu. Sodinokibi Ransomware Hits New York Airport Systems. *Bleeping Computer.* [Online] 10 January 2020. https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/.

18. Asokan, Akshaya. Albany Airport Pays Off Sodinokibi Ransomware Gang: Report. *Bank Info Security.* [Online] 13 January 2020. https://www.bankinfosecurity.com/albany-airport-pays-off-sodinokibi-ransomware-gang-report-a-13602.

19. Gallagher, Sean. Spanish Companies' Networks Shut Down as Result of Ransomware. ***ARS Technica.*** **[Online] 4 November 2019. https://arstechnica.com/information-technology/2019/11/spanish-companies-networks-shut-down-as-result-of-ransomware/.**

20. Naymik, Mark. Cleveland Breaks Silence On Airport Ransomware Attack. ***Government Technology.*** **[Online] 29 April 2019. https://www.govtech.com/security/Cleveland-Breaks-Silence-on-Airport-Ransomware-Attack.html.**

21. European Parliament and Council of European Union. ***General Data Protection Regulation (EU) 2016/679.*** **14 : April, 2016.**

22. ***Directive 95/46/EC of the European Parliament and of the Council.*** **The European Parliament and the Council of the European Union. 1995, Official Journal of the European Union, p. 31-50.**

23. International Organization for Standardization. ISO/IEC 27001 Information Security Management. ***ISO.*** **[Online] 21 January 2020. https://www.iso.org/isoiec-27001-information-security.html.**

24. International Civil Aviation Organization. ***Convention of International Civil Aviation.*** **2006.**

25. (ICAO), International Civil Aviation Organization. Annex 17 to the Convention of International Civil Aviation. ***Safeguarding International Civil Aviation Against Acts of Unlawful Interference.*** **March 2011.**

26. Spit, Marcel. Universal Security Management Systems Standard 2017. [Online] https://www.adviescentrumbvi.nl/usms-2017/.

27. ***Council Directive 2004/82/EC.*** **The Council of the European Union. 2004, Official Journal of the European Union.**

28. ***Regulation (EC) No 300/2008 of the European Parliament and of the Council.*** **The European Parliament and the Council of the European Union. 2008, Offical Journal of the European Union, p. 72-84.**

29. Council, European. ***Overview of Natural and Man-made Disaster Risks the European Union may face.*** **2014.**

30. ENISA. ***ECI Directive: Proposal for a Directive of the Council on the Identification and Designatio of European Critical Infrastructure and the assessment of the need to improve their protection.*** **Brussels : s.n., 2006.**

31. Marianthi Theocharidou, Georgios Giannopoulos. ***Risk assessment methodologies for critical infrastructure protection. Part II: A new approach.*** **2015.**

32. Giannopoulos, Georgios, Filippini, Roberto e Schimmer, Muriel. ***Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.*** **s.l. : Publications Office of the European Union, 2012.**

33. DHS. National Infrastructure Protection Plan - Partnering to enhance protection and resiliency. ***DHS.*** **[Online] 2009. [Riportato: 02 11 2020.] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiQwra8o-bsAhVhpYsKHRy9DtAQFjAAegQIARAC&url=https%3A%2F%2Fwww.dhs.gov%2Fxlibrary%2Fassets%2FNIPP_Plan_noApps.pdf&usg=AOvVaw1abe9KlMuVEcSQIb_mbXH_.**

34. LA MÉTHODE EBIOS RISK MANAGER. LA MÉTHODE EBIOS RISK MANAGER. [Online] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/.

35. ***The bowtie method: A review.*** **de Ruijter, A. e Guldenmund, F. October 2016, Safety Science, Vol. 88, p. 211-218.**

36. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation). ***CioWiki.*** **[Online] 18 December 2019. [Riportato: 11 November 2020.] https://cio-wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation).**

37. Luyten, Denis. ***SECUR-ED Risk Assessment guidelines for Public Transport.*** **Estoril, Portugal : NFPA-APSEI Fire & Security conference, 2012.**

38. Naymik, Mark. Cleveland Acknowledges for First >Time Hopkins Airport Hack Involved Ransomware. ***Cleveland.*** **[Online] 29 April 2019. https://www.cleveland.com/news/2019/04/cleveland-acknowledges-for-first-time-hopkins-airport-hack-involved-ransomware.htm.**

39. SATIE project. ***D2.5 - Specification of the impact propagation model.*** **2020.**

40. Osborne, Charlie. Chinese hackers take down Vietnam airport systems. ***ZDNet.*** **[Online] 1 August 2016. [Riportato: 6 October 2020.] https://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/.**

41. Spit, Marcel. Universal Security Management Systems Standard 2017. [Online] https://www.adviescentrumbvi.nl/usms-2017/.

42. SATIE project. ***D2.4 Specification of a holistic security management cycle.*** **2020.**

43. European Parliament and Council. ***Data Protection Directive 95/46/EC.*** **24 : October, 1995.**

7 Annex 1 - Threats included in the risk assessment

The following table lists all the included threats in the risk analysis.

Table 7.1: Threats included in the risk assessment

Macro-Category	Threat Category	Threat	Threat Description
Safety	Accidental Conducts or Accidental Situations	Crowd in panic	An unmanageable crowd which, in panic, can hurt people.
Safety	Accidental Conducts or Accidental Situations	Developer Mistake	Loss of data integrity or service availability as a result of developer mistakes
Safety	Accidental Conducts or Accidental Situations	Errors in Exercise of Personal Data Subject Rights	Errors in the exercise of the rights of interested parties regarding the processing of personal data
Safety	Accidental Conducts or Accidental Situations	Lack of Personnel	The number of workers is reduced on the basis of prolonged absences for any reason (illness, accident, maternity, etc..) or for dismissal
Safety	Accidental Conducts or Accidental Situations	Maintenance Error	Loss of data integrity or service availability due to errors committed by maintenance personnel qualified to work on specific systems or applications
Safety	Accidental Conducts or Accidental Situations	Non Conformity to Mandatory Laws and Standards	Non-compliance of policies and corporate security requirements
Safety	Accidental Conducts or Accidental Situations	Non-Compliance with Corporate Security Policies	The failure to meet legal requirements with the consequent risk of running into administrative or criminal penalties
Safety	Accidental Conducts or Accidental Situations	Operator Mistake	Loss of data integrity or service availability due to errors committed by operators authorized to operate on specific systems or applications
Safety	Accidental Conducts or Accidental Situations	Personnel Tiredness-Stress	Loss of data integrity or service availability due to errors, inaccuracies or misstatements committed by personnel involved in operations on the systems and applications with medium-high privilege levels
Safety	Accidental Conducts or Accidental Situations	Reduced or Absent Technical Skills	Skills residing in few people or a threat of loss of any type of personnel with specific skills (through quitting, maternity leave, etc.)
Safety	Accidental Conducts or Accidental Situations	System Analyst Error	Loss of data integrity or service availability due to errors committed by personnel qualified to install, configure and maintain - directly or indirectly - systems, applications or proprietary systems
Safety	Environmental Causes	Air Conditioning Malfunctioning	Destruction or damage of a system or a part of it as a consequence of the monitoring/control system malfunctioning due to temperature and/or humidity.
Safety	Environmental Causes	Dust Particles	Damage of a system or of a part of it and/or loss/modification of data as consequence of dust deposit and/or particles capable of causing destructive micro short circuits in the electronic circuit boards that make up the system

Macro-Category	Threat Category	Threat	Threat Description
Safety	Environmental Causes	Electromagnetic Interference (EMI)	Hardware device interference produced by electromagnetic radiation and consequent loss/modification of processed, stored, or in-transit data.
Safety	Environmental Causes	Heavy Voltage Reduction (brownout)	Inability of the companies that supply voltage to provide the service within an acceptable range (e.g. 200-240 volts) that may cause problems on electrical components including reducing their life cycle or damaging them permanently
Safety	Environmental Causes	Inadequate Microclimate Environment	Unavailability of drinking water, necessary to ensure the hygienic conditions of the rooms and offices; uncomfortable climate in terms of ventilation, lighting, etc..
Safety	Environmental Causes	Lack of Electric Current (blackout)	The power devices may be interrupted in their operation, causing loss/modification of the processed data besides data unavailability
Safety	Environmental Causes	Minimums, Peaks and Surges	Temporary or rapid voltage level changes and surges that can cause operation system interruptions and/or processed data loss/modification besides their unavailability.
Safety	Environmental Causes	Nuclear radiation	It refers to a nuclear accident with consequences on infrastructure and people
Safety	Natural Causes	Bad Weather Conditions	Destruction of a system or a part of it as a consequence of hurricanes, tornadoes, snow storms, or any other high-intensity storms.
Safety	Natural Causes	Earthquake	Destruction of a system or a part of it as a consequence of tectonic movements
Safety	Natural Causes	Epidemic	Epidemic contagion within the company staff that affects their activities for a significant period of time
Safety	Natural Causes	Fire	Fire in the rooms where the system, its memory, or any paper with data on it are located.
Safety	Natural Causes	Flooding	Flooding of the rooms where the system and/or media storage is located (due to pipes or fixtures breaking).
Safety	Natural Causes	inability to use the enrolled credentials to login	A user, for some reason, cannot use the enrolled biometric elements to authenticate themself.
Safety	Natural Causes	Jumps in Temperature or Humidity	Destruction or damage of a system (or a part of it) as a consequence of jumps in temperature in the room where the system and/or its memory is located.
Safety	Natural Causes	Lightning	Destruction of a system or a part of it as a consequence of a lightning strike.
Safety	Natural Causes	Pandemic	Global pandemic contagion that affects the organization's business and its relations with the commercial world

Macro-Category	Threat Category	Threat	Threat Description
Safety / Security	Organizational Events	Lost	A physical asset is lost.
Safety / Security	Organizational Events	Undefined Internal Roles and Responsibilities	Functional charts and organizational charts incorrectly defined or lacking mapped responsibilities within the organization
Safety / Security	Safety Accidents	Hardware Malfunctioning Repetition	Situations in which the same type of incident is repeated on the same asset continuously
Safety / Security	Safety Accidents	Repetition of Anomalies Related to Personnel Mistakes	Personnel repetition of activities which involve errors or anomalies or situations that do not conform with the policies and procedures
Safety / Security	Technical Causes	Application Software Malfunctioning	Unavailability, loss and/or modification of processed or in-transit data due to an application software malfunctioning
Safety / Security	Technical Causes	Basic Software Malfunctioning	Unavailability, loss and/or modification of processed or in-transit data due to an operating system and third-party software malfunctioning
Safety / Security	Technical Causes	Communication Equipment Failure	Loss of data and service availability as a consequence of communication equipment malfunction or failure.
Safety / Security	Technical Causes	Error in detecting danger/violation (false negatives)	The failure (human or machine) in detecting danger or a violation of an object.
Safety / Security	Technical Causes	Forbidden Access to Network, Basic Software, Applications	Loss of data confidentiality, integrity and availability as a result of unauthorized access (voluntary or involuntary) to the telecommunication network (sharing), basic software and/or applications
Safety / Security	Technical Causes	Forbidden Access to Storage Devices	Loss of confidentiality, integrity and availability of data as a consequence of unauthorized access (voluntary or involuntary) to storage devices
Safety / Security	Technical Causes	Hardware Malfunctioning	Unavailability, loss and/or modification of processed or in-transit data as a consequence of hardware malfunctions of the system or parts of it.
Safety / Security	Technical Causes	Logic Bomb, Trap Doors	Code portions included in the system which, when triggered by particular events, perform destructive actions on the data, applications, and/or systems
Safety / Security	Technical Causes	Malware Software (Virus, Worm, Trojan, etc.)	Software created with the only purpose of causing damage, more or less extended to the systems on which it runs automatically (worms) or unknowingly by users (Virus, Trojan)
Safety / Security	Technical Causes	Message Routing Problems	Loss of confidentiality, integrity and availability of data as a consequence of routing problems of the traffic to and from the source(s) to the legitimate destination(s)

Macro-Category	Threat Category	Threat	Threat Description
Safety / Security	Technical Causes	Network Overload	Unavailability, loss and/or modification of data in transit due to network data transport overload
Safety / Security	Technical Causes	Personal Data Breach	An uncontrolled personal data breach during the processing of personal data
Safety / Security	Technical Causes	Storage Media Deterioration	Loss of data and services availability as a consequence of deterioration/breakdown of storage media
Safety / Security	Technical Causes	Theft (Data breach)	Misappropriation of data for fraudulent and illegitimate purposes, in order to cause various kinds of damage, such as the unavailability of data and services, the theft of data or unauthorized access.
Safety / Security	Technical Causes	Utility Malfunctioning	Loss of data and service availability as a consequence of the utility malfunctioning
Safety / Security	Third Parties Report	Not Supported Basic Software	Situations where the vendor does not provide support and patches for the operating system version
Safety / Security	Third Parties Report	Not Supported Third-party Software	Situations in which providers do not supply patches or changes to the application software
Safety / Security	Third Parties Report	Supplier Unavailability	Situations in which the suppliers are not able to hold down services as a result of strikes, reduced staff or deliberate actions
Security	Terrorism and Sabotage	Abusive Entrance (Piggyback, Tailgating)	Illegal access to a system by "tagging along" with an authorized person
Security	Terrorism and Sabotage	Bomb	Destruction of the system or parts of it, storage systems and equipment following the explosion of bombs or other material which could cause explosions
Security	Terrorism and Sabotage	Communication Infiltrations	Unauthorized entry into the communication between two or more parties (Man-in-the-middle) for the purposes of espionage or data theft
Security	Terrorism and Sabotage	Denial of Service (DoS)	Unavailability of an access service by users, applications and networks
Security	Terrorism and Sabotage	False Information Insertion	Inserting incorrect information into a system by authorized personnel
Security	Terrorism and Sabotage	Hijacking	A vehicle (or airplane) is hijacked, including to the wrong gate. This could also happen by tampering information sent to the driver/pilot.
Security	Terrorism and Sabotage	Information Management Equipment Tampering	Impairment of the integrity, availability and confidentiality of processed or in-transit data through equipment tampering or system tampering
Security	Terrorism and Sabotage	Intimidation	Theft of credentials or data and/or unauthorized access to systems and rooms by techniques of coercion or extortion (even through practices of social engineering)

Macro-Category	Threat Category	Threat	Threat Description
Security	Terrorism and Sabotage	Masquerading	Masquerading of a person who provides a false identity to a system in order to earn unauthorized access
Security	Terrorism and Sabotage	Melee attack	Any combat which involves directly striking a person at a range of less than a meter, especially using a meter, especially using martial arts or a melee weapon such as knives, etc.
Security	Terrorism and Sabotage	Physical attack and consequent unauthorized access to the secured zone	Any kinds of physical attack that aims to break a barrier by a physical attack (bombing, striking with a heavy vehicle, etc.).
Security	Terrorism and Sabotage	Scavenging	Scavenging information (discs, records, tapes) to gain access to the system and/or rooms
Security	Terrorism and Sabotage	Technological Equipment Tampering	Impairment of technological equipment functioning (air conditioning, fire sprinkler systems, access control)
Security	Terrorism and Sabotage	Unnoticed Data Subtraction (Salami Attack, Rounding)	Collecting of information in very small quantities in an unnoticed way, even by using Trojan Horse
Security	Terrorism and Sabotage	Vehicle-ramming attack	A vehicle-ramming attack is an assault in which a perpetrator deliberately rams a vehicle into a building or crowd of people.
Security	Terrorism and Sabotage	Wiretapping	Wiretapping of electromagnetic waves or telecommunication cables for the purposes of espionage or involuntary wiretapping of wires and cables during maintenance work.
Security	Voluntary Conducts	Compromised people (cyber, no security clearance)	Compromised people with no clearance seek to create cyber damage to the organization through malicious actions on cyber assets
Security	Voluntary Conducts	Compromised people (physical, no security clearance)	Compromised people with no clearance seek to create physical damage to the organization through malicious actions on physical assets
Security	Voluntary Conducts	Compromised personnel (cyber, high security clearance)	Compromised personnel with high clearance seek to create cyber damage to the organization through malicious actions on cyber assets
Security	Voluntary Conducts	Compromised personnel (cyber, medium security clearance)	Compromised personnel with medium clearance seek to create cyber damage to the organization through malicious actions on cyber assets
Security	Voluntary Conducts	Compromised personnel (physical, high security clearance)	Compromised personnel with high clearance seek to create physical damage to the organization through malicious actions on physical assets

Macro-Category	Threat Category	Threat	Threat Description
Security	Voluntary Conducts	Compromised personnel (physical, medium security clearance)	Compromised personnel with medium clearance seek to create physical damage to the organization through malicious actions on physical assets
Security	Voluntary Conducts	False enrolment	When a system is initialized with false biometric credentials that pertain to the attacker and not to the legitimate person whose account is being enrolled in the system.
Security	Voluntary Conducts	Listening to Unauthorized Communications	Voluntary or involuntary listening to confidential information
Security	Voluntary Conducts	Repudiation	Possibility that a particular sender of a generic message (email, IP packet, ticket, etc.) may afterwards deny having sent the message itself. The sender can be represented by an individual but also by an application
Security	Voluntary Conducts	Social Engineering	An attacker uses social engineering techniques to gain access to confidential information (in read/write or read only) or to restricted areas
Security	Voluntary Conducts	Theft (Physical)	Misappropriation of hardware, software, or equipment for fraudulent and illegitimate purposes, in order to cause various kinds of damage, such as the unavailability of data and services, the theft of data or unauthorized access.
Security	Voluntary Conducts	Unauthorized Access to Physical Areas	Unauthorized access gained to the building in a fraudulent way
Security	Voluntary Conducts	Unauthorized Network and Resource Use	Fraudulent and unauthorized use of network telecommunications with a consequent deterioration of the availability of resources and a decline in the service level provided and resource performance available.
Security	Voluntary Conducts	Unauthorized Software Use	Loss of data integrity and confidentiality as a result of unauthorized use of software, including misuse and abuse, not in line with the company's policy (which risk damages, including financial, reputational, physical, etc.)
Security	Voluntary Conducts	Unauthorized storage device use	Unauthorized use of storage devices for purposes of data theft
Security	Voluntary Conducts	Wrongful Use of Company Software	Software use for wrongful or purposes other than those permitted and approved by the company and/or the organization's policy

8 Annex 2 - Vulnerabilities included in the risk assessment

The following table lists all the included vulnerabilities in the risk analysis.

Table 8.1: Vulnerabilities included in the risk assessment

Vulnerability Category	Vulnerability	Vulnerability Description
Access Control	Change of a biometric element	It refers to the case when a biometric element changes over time (for example a fingerprint can change due to a scar)
Access Control	Inadequate Credentials Management	Refers to the lack of controls and/or the inadequacy in the management of the access credentials to IT resources
Access Control	Insufficient Identification of Errors in Logical Access Management	Refers to the lack of mechanisms, systems and organizational/operational procedures for error identification and management of systems, applications and business processes
Access Control	Lack of Assignment of Roles and Tasks	Refers to the lack of a clear assignment of responsibilities and duties within the services
Access Control	Lack of Audit Trail	Refers to the lack or faulty management of the traces of user access authentication and authorization. As a rule, the optimal management of log records and audit trail should allow for the reconstruction of login events at any given moment
Access Control	Lack of Correct Transmission Reports of Messages/Data	Refers to the lack of mechanisms or procedures to confirm the correct transmission/reception of messages and data between two or more correspondents
Access Control	Mismanagement of Privileges	Refers to the lack of controls and/or the inadequacy in the management of user access privileges to IT resources
Access Control	Unsuitable Application Authentication Mechanisms	Refers to the inefficiency or unsuitability of the authentication mechanisms enabled on the application, in order to properly manage the recognition of users/operators, applying the appropriate access privileges
Administrative Management	Lack of Procedures for Change Management	Refers to the absence of or inadequacy of procedures for change management, which includes the entire lifecycle of a system, an application or a process (design, testing, implementations)
Compliance Management	Lack of Tools for the Software Configurations Control	Refers to the lack of software tools and/or organizational and operational procedures that allow for the control and monitoring of the compliance of software configurations of the systems with the corporate security policies
Compliance Management	Lack of Tools for the Verification of Compliance with Mandatory Standards	Refers to the lack of software tools and/or organizational and operational procedures that allow for the control and monitoring of the compliance of the whole organization with laws.
Computer and Network Management	Bugs in Operating Systems	Refers to the presence of defects and/or errors within the operating systems that are not addressed through proven organizational and operational procedures, able to apply speedy fixes and patches (when available)

Vulnerability Category	Vulnerability	Vulnerability Description
Computer and Network Management	Inadequacy of Authentication Mechanisms for Access from External Networks	Refers to the absence of or inadequacy of the system to recognize, identify and authenticate users operating with connections from poorly-controlled external networks (untrusted) and not compliant to the internal security policy
Computer and Network Management	Insufficient Segregation of Logic Areas of Work	A "logical area of work" means an area logically defined in the system accessed by users. The vulnerability refers to the lack or shortage in the definition of the boundaries of these logical areas
Computer and Network Management	Lack of Confidentiality Clauses in Contracts	Refers to the additional conditions to be included in contracts with suppliers and customers
Computer and Network Management	Lack of Controls on the Flow of Information	Refers to the lack of control on the information flow on transport networks (wired or wireless), for example, the lack of mechanisms/systems of traffic control (firewall) or the use of unencrypted protocols
Computer and Network Management	Lack of Logging Security Events	Situations in which events that may impact the information security are not properly tracked and their management is not recorded (learning from accidents)
Computer and Network Management	Lack of monitoring of the worn down devices	It is the case in which worn equipment is not adequately monitored and replaced and/or the instructions for maintenance and rotation of the equipment are not followed, as required by the manufacturers
Computer and Network Management	Lack of Overloaded Network Management	Refers to the inadequacy to predict/detect in advance the increase in demand for data/information in transit on systems or network appliances, to respond with appropriate measures
Computer and Network Management	Lack of Redundancy of Communication Networks	Refers to the absence or lack of alternative systems of communication that provide the continuity of the transport service of the telecommunication network, even if failures occur in the main line
Computer and Network Management	Lack of Segregation Among System Applications	Refers to situations where the application server and the web server are not segregated by a demilitarized zone (DMZ)
Computer and Network Management	Lack of Traceability of Operations Carried Out on Applications	Access to applications is made through a shared password
Computer and Network Management	System Clocks not Synchronized	Refers to the lack of synchronization of the system clocks, normally achieved by the use of a hierarchy (stratum) of servers that synchronizes all systems using Network Time Protocol (NTP)
Computer and Network Management	Unencrypted Credentials	It is the case in which, during the authentication, user credentials (for example a user ID and password) are unencrypted and thus exposed to the threat of interception
Computer and Network Management	Unprotected Connections to Public Networks	Refers to the absence or lack of control on the connections to and from public networks (e.g. internet)
Computer and Network Management	Unprotected Lines of Communication	Refers to the shortage or absolute lack of protection systems of lines of communication (wired or wireless)

Vulnerability Category	Vulnerability	Vulnerability Description
Computer and Network Management	Unsafe Password Management for accessing Customer DB	Refers to the convention adopted for the password setting used to login to the DB
Environmental Security	Access to Offices not Allowed	It is the case in which for any reason (weather conditions, riot, sabotage, etc.) you cannot access the premises
Environmental Security	Buildings not Protected from Explosion	It is the case in which buildings, environments or equipment rooms do not ensure adequate protection against explosions both intentional (e.g. bombs) and accidental (e.g. lightning, gas leak due to human incompetence)
Environmental Security	Inadequate Revisions to Physical Security Systems	Refers to the maintenance of smoke detectors, fire sprinklers, fire extinguishers, etc. (according to the safety standards required by Law n°626)
Environmental Security	Office Destruction	Physical destruction of the offices with the complete absence of workability
Environmental Security	Susceptibility of the Equipment to fluctuations of electricity and non-stabilized power supply	Refers to the degree of sensitivity and possible intolerance of the equipment to operate with maximum and minimum variations of the electricity and the electric power supply does not guarantee a well determined and constant level of voltage
Environmental Security	Susceptibility of the Equipment to Humidity/Temperature	Refers to the degree of sensitivity and possible intolerance of the equipment to operate at maximum and minimum levels of the percentage of humidity and temperature in the surrounding environment
Environmental Security	Systems Unprotected from Electrostatic Discharge	Refers to the inadequacy of protection relating to electrostatic discharge, such as the lack of grounding of electrical devices to prevent the accumulation of static electricity and the static discharge causing damage
Environmental Security	Unprotected Removable Storage Devices	It is the case in which storage and backup removable devices are not adequately protected from possible theft, breaches, tampering, modification and damage. In this case the term "protection" refers to physical protection
Environmental Security	Worn down equipment not replaced	It is the case in which worn equipment is not adequately replaced and/or the instructions for maintenance and rotation of the equipment are not followed, as required by the manufacturers
Environmental Security	Worn Storage Devices not Replaced	It is the case in which worn storage devices are not adequately replaced and/or the instructions for maintenance and rotation of the devices are not followed, as required by the manufacturers
Operation Management	Absence of/reduced rules for application of personal data subject rights	Situations where there are not enough instructions and procedures to appropriately manage the application of personal data subject rights (deletion, restriction, portability….)

Vulnerability Category	Vulnerability	Vulnerability Description
Operation Management	Communication issues between the Airport's Operation Centre and police authorities	Terminal areas accessible to the public (passengers and other people) cannot be patrolled continuously due to communication issues occurring often between the Airport's Operation Centre and the relevant authorities (e.g. police centre) for a timely response. These inadequate traffic arrangements result in a crowded and chaotic circulation of vehicles and people outside of the terminals
Operation Management	Complex User Interfaces	Refers to the possibility that the management interfaces of the systems are not sufficiently simple and intuitive. This could involve incorrect or imprecise configurations with a resulting degradation of security systems
Operation Management	Lack of Assistant Turnover	Assistants that manage the same customer for a long time
Operation Management	Lack of Personnel	Refers to the inadequacy of human resources in order to operate, manage, maintain, support and monitor the general system
Operation Management	Lack of Physical Protection of Archives	Refers to the hardcopy archive (a cabinet containing significant paper documents)
Operation Management	Lack of screening machines	It refers to the fact that the access to a certain area is not monitored by screening machines (e.g. explosive detection machines, metal detectors, radioactive material detectors, etc.)
Operation Management	Lacking Control in the Transfer Management of Technical Information with Customers	Refers to the exchange by e-mail, or through other electronic forms, of the request for credential creation and operational management between operators and users
Operation Management	Lacking Data Deletion on Reused Devices	Refers to the lack of planned secure data deletion from decommissioned and reused devices (disks, tapes, memories). This could involve an involuntary loss of confidentiality of information
Operation Management	Lacking Process of Configuration Management	Refers to the lack of procedures and/or processes for the protection of devices and system configurations so that configurations lifecycle is protected and their appropriate storage guaranteed.
Operation Management	Lacking Process of Defect Detection in Software	Refers to the lack of optimized procedures and processes (testing, monitoring) for the detection of defects in software and applications.
Operation Management	Loss of Historical Information Related to the Type of Service Configuration	Situation in which there is no tracking of system configurations or their changes
Operation Management	Missing update when new elusion technique are discovered	It refers to the case in which an update is not carried out when new techniques are discovered to cause false negatives
Operation Management	Not updated security documentation	The security door inspection records aren't adequately retained or updated.
Operation Management	Outdated Application Software	The application software is not properly supported by suppliers

Vulnerability Category	Vulnerability	Vulnerability Description
Operation Management	Outdated Operating Systems	Situations where system patches and upgrades of the service pack have not been correctly applied
Operation Management	Reduced capabilities in incident detection for personal data processing	Reduced approach, culture, tools and instructions about the timely detection of a personal data breach
Operation Management	Reduced Protection for Access to Applications	Refers to conventions in the creation of passwords for administrator access to applications (weak password)
Operation Management	Reduced Segregation of UI	Refers to poor management of pages on applications that are accessed by operators, sometimes simultaneously
Operation Management	Reduction of Provided Service Levels	Situations in which the service provided by the staff is not compliant with the expected levels
Operation Management	Untested Machine	It refers to the case in which periodic tests are not carried out to verify if the device works correctly (during commissioning and periodically during the device lifecycle)
Operation Management	Untested Software Applications	It is the case in which procedures for testing software and applications before being put into production are not planned
Organizational Management	Bad labour conditions	It refers to the case when airport employees are disgruntled or dissatisfied for monetary or idealistic reasons (e.g. low salaries, unachieved personal ambitions, trends to radicalism) or unintentionally (e.g. lack of targeted training courses), resulting in them not being motivated in their role/contribution to protect human life.
Organizational Management	Corruption (external)	Corruption of personnel external to the organization (third parties, maintainers, outsourcers)
Organizational Management	Corruption (internal)	Corruption of personnel within the organization
Organizational Management	Incomplete Security Specifications	It is the lack or shortage of security specifications included in system requirements and in general in information infrastructure, both in their development phase and in the next phase of management, control and maintenance.
Organizational Management	Lack of a uniform security policy for physical access control	Lack of a uniform policy and procedure for controlling physical access to work areas and to hardware (computers, communication devices, etc.) and software media
Organizational Management	Lack of adequate police at security screening checkpoints	Lack of adequate police forces for the protection of the checkpoints, for passengers and non-passengers, and thus sufficient support for the prevention of security breaches is not possible.
Organizational Management	Lack of appropriate staff to check the CCTV	The CCTV system of some sectors isn't monitored by appropriate, designated personnel
Organizational Management	Lack of approval process	Absence of a formal approval process for decision making
Organizational Management	Lack of communication and involvement of interested parties	Situations where stakeholders and involved people are not updated or communication is not shared with them

Vulnerability Category	Vulnerability	Vulnerability Description
Organizational Management	Lack of coordination between business and IT areas	Situations where processes, information and strategic objectives are not shared between business and IT areas
Organizational Management	No provision for sufficient background check for airport ID issuance	Lack of sufficient background checking before issuing an airport ID for any reason (e.g. lack of funds, personnel, etc.).
Organizational Management	Procedural issues in hazardous goods and material inspection	The procedures for maintaining and updating hazardous goods and hazardous material records aren't clear
Organizational Management	Reduced approach for continual improvement	Reduced attention to evaluate results of performance in order to improve services to customers and create a good relationship with the stakeholder
Organizational Management	Reduced involvement of operational staff	Refers to the absence or reduced sharing of status, trend and any information about performance of the service with operating and technical people
Organizational Management	Unguarded Barrier	In refers to the case in which barriers are not guarded by surveillance personnel, nor periodically and randomly patrolled
Personnel Management Security	Inappropriate Hiring Procedures	Refers to the lack or total absence of procedures to select new candidates, based on personal reminder (crimes, morality, expertise) and that related to security (background screening)
Personnel Management Security	Incorrect/Non-Compliant Use of Information	It is the possibility of an incorrect use (intentional or accidental) of information handled by users
Personnel Management Security	Lack of Authentication Mechanisms on the Systems	Refers to the absence of or inadequacy of the system to recognize, identify, and authenticate users operating on different systems. The lack of unambiguous authentication of personnel operating on systems does not allow for the identification of all system accesses
Personnel Management Security	Lack of Automatic Logout	Refers to the absence of controls, rules and specific configurations that allow the automatic ending of sessions in the case of prolonged inactivity
Personnel Management Security	Lack of Control and Supervision of Cleaning Staff	Refers to the inadequacy or absolute lack of control and monitoring of the activities of cleaning personnel in spaces, buildings and premises of the organization
Personnel Management Security	Lack of Documented Operating Procedures	Refers to the lack or shortage of documents and guidelines detailing operating procedures for the development, management, control, maintenance, revision and monitoring of systems
Personnel Management Security	Lack of Emergency Procedures	Refers to the lack of emergency procedures approved, in writing or verbally. This scope covers both the procedures related to the systems and those for personnel security.
Personnel Management Security	Lack of Policies for Communications Usage	It is the lack or absence of clear rules and procedures for the use of communications related to both telecommunications network voice and/or data (phone or computer network), and conventional communications among people (e.g., dialogues, notes)
Personnel Management Security	Lack of Policies for Resources Usage	It is the lack or absence of clear rules for the general use of information resources whether they refer to the network, systems or applications

Vulnerability Category	Vulnerability	Vulnerability Description
Personnel Management Security	Lack of Security Awareness	Refers to the absence or lack of initiatives, training and specific training phases, necessary to increase users' awareness on the issues of security, on the organizational aspects of relevance, on policies and procedures
Personnel Management Security	Lack of Supervision in Carrying out Operational Work	Refers to the inadequacy or absolute lack of control, management and monitoring of the activities of personnel involved in various operational functions
Personnel Management Security	Poorly-trained Staff	Refers to the absence or lack of planned staff training and/or exercises with the aim of optimizing the use of resources and to make all users aware of the rules to be observed in different areas
Personnel Management Security	Untested Emergency Procedures	Refers to the lack of evidence (simulations), verifications and checks of the validity of the emergency procedures
Physical Security	Hardware Devices not Physically Protected	Refers to the absence or lack of systems for the physical protection of hardware devices, such as unlocked technical cabinets (rack)
Physical Security	Inadequate Access Control to CED	Refers to the lack of or inadequacy of controls on the access of people to datacentres and equipment rooms. As a rule, controls can be carried out through security doors, locks, badges, access logs, etc.
Physical Security	Inadequate Access Control to Operating Area	Refers to the lack of or inadequacy of controls on the access of people in the operational areas (linked to the main/critical production processes). As a rule, controls can be carried out through security doors, locks, badges, access logs, etc.
Physical Security	Inadequate barrier	It refers to the case in which physical barriers are not hardened or robust
Physical Security	Inadequate CCTV cameras surveillance equipment at entry/exit points	Inadequate CCTV camera surveillance equipment at entry/exit points that lead to security controlled areas, such as but not limited to doors, gates, barriers and any other kind of passage.
Physical Security	Inadequate maintenance of CCTV cameras	Inadequate maintenance of CCTV cameras and emergency buttons results in inefficient monitoring, facilitating screening control deviation at entry / exit points that lead to security controlled areas, such as but not limited to doors, gates, barriers and any other kind of passage.
Physical Security	Inadequate number of personnel at security controlled areas	Due to the inadequate number of personnel, double-checking procedures of the staff requiring access into security-controlled areas or providing goods and services within these areas could not be supported. As a result, the respecting sensitive documentation access into security-controlled areas could not be inspected properly.
Physical Security	Incapable power supply	This refers to the case when power has fluctuations.
Physical Security	Insufficient capacity	It refers to the case when a closed location cannot contain the number of people needed during a particular event

Vulnerability Category	Vulnerability	Vulnerability Description
Physical Security	Insufficient property perimeter security	Lack of appropriate perimeter protection (i.e. the perimeter should be fenced against vehicles, via a standard chain-link fence with razor barbed wire, smart cameras installed at certain locations to detect irregular movement along the perimeter, supervision at all gates, and requiring manual opening of gates at least frequently used gates).
Physical Security	Insufficient protection of the litter bins	Refers to vulnerabilities related to using unprotected and unlocked litter bins, or using opaque bins which make it easier to hide a large timer or remote radio-controlled IED (improvised explosive device).
Physical Security	Lack of anti-intrusion systems at barriers	In refers to the case in which barriers don't have an intrusion detection system so that a security violation is detectable, at least ex-post facto.
Physical Security	Lack of explosive detection systems that allow for the detection of Vehicle Born Improvised Explosive Devices (VBIEDs)	VBIEDs may need special detectors positioned in specific places to be avoided. VBIEDs do not result in major structural damage but can cause extensive business interruption, potential loss of life, and often irreparable damage to the brand image.
Physical Security	Lack of Landside Security Monitoring	It refers to vulnerabilities related to the lack of patrolling or behavioural analysis training for security staff for landside security monitoring. Landside security responsibility normally lies under federal and regional police control.
Physical Security	Lack of Physical Access Controls (Office)	Refers to the lack of access control for people in offices and workplaces. As a rule, controls can be carried out through closed doors, keys, badges, access logs, security guard services, cameras, etc.
Physical Security	Missing control at boundaries between different security zones	It refers to the case when boundaries between zones that have different security levels (such as airside and landside) are of less frequent security patrolling than required. Therefore, inspection at regular and irregular intervals in that area is not carried out and passage through such boundaries are unprotected.
Physical Security	Missing isolation between pilots/drivers and passengers	It refers to the case when the pilot can be physically reached by a passenger, who can threaten the pilot
Physical Security	Passengers Screening outside Terminal Building	Vulnerabilities from a lack of or weak passenger screening outside he terminal building (e.g. enhanced profiling of passengers, the presence of explosive detection dogs)
Physical Security	Surveillance issues regarding vehicle entrance permits and/or checks	It refers to the case when inadequate training of the airport security staff (i.e. training courses not updated according to international developments in the field of aviation security), concerning the vehicle checking procedures, which leads to the lack of sufficient supervision. Thus, vehicles needing to move between landside and airside areas pass the check point procedure easily without being requested to provide the appropriate permission.

9 Annex 3 - Security controls

The following table lists all the security controls included in the risk analysis.

Table 9.1: The exhaustive list of controls included in the risk assessment

Control Domain Code	Control Domain Name	Control Code	Control Name
A.5.1	MANAGEMENT DIRECTION FOR INFORMATION SECURITY	A.5.1.1	Policies for information security
		A.5.1.2	Review of the policies for information security
A.6.1	INTERNAL ORGANIZATION	A.6.1.1	Information security roles and responsibilities
		A.6.1.2	Segregation of duties
		A.6.1.3	Contact with authorities
		A.6.1.4	Contact with special interest groups
		A.6.1.5	Information security in project management
A.6.2	MOBILE DEVICES AND TELEWORKING	A.6.2.1	Mobile device policy
		A.6.2.2	Teleworking
A.7.1	PRIOR TO EMPLOYMENT	A.7.1.1	Screening
		A.7.1.2	Terms and conditions of employment
A.7.2	DURING EMPLOYMENT	A.7.2.1	Management responsibilities
		A.7.2.2	Information security awareness, education and training
		A.7.2.3	Disciplinary process
A.7.3	TERMINATION AND CHANGE OF EMPLOYMENT	A.7.3.1	Termination or change of employment responsibilities
A.8.1	RESPONSIBILITY FOR ASSETS	A.8.1.1	Inventory of assets
		A.8.1.2	Ownership of assets
		A.8.1.3	Acceptable use of assets
		A.8.1.4	Return of assets
A.8.2	INFORMATION CLASSIFICATION	A.8.2.1	Classification of information
		A.8.2.2	Labelling of information
		A.8.2.3	Handling of assets
A.8.3	MEDIA HANDLING	A.8.3.1	Management of removable media
		A.8.3.2	Disposal of media
		A.8.3.3	Physical media transfer
A.9.1	BUSINESS REQUIREMENTS OF ACCESS CONTROL	A.9.1.1	Access control policy
		A.9.1.2	Access to networks and network services
A.9.2	USER ACCESS MANAGEMENT	A.9.2.1	User registration and de-registration
		A.9.2.2	User access provisioning
		A.9.2.3	Management of privileged access rights
		A.9.2.4	Management of secret authentication information of users
		A.9.2.5	Review of user access rights
		A.9.2.6	Removal or adjustment of access rights

Control Domain Code	Control Domain Name	Control Code	Control Name
A.9.3	USER RESPONSIBILITIES	A.9.3.1	Use of secret authentication information
A.9.4	SYSTEM AND APPLICATION ACCESS CONTROL	A.9.4.1	Information access restriction
		A.9.4.2	Secure log-on procedures
		A.9.4.3	Password management system
		A.9.4.4	Use of privileged utility programs
		A.9.4.5	Access control to program source code
A.10.1	CRYPTOGRAPHIC CONTROLS	A.10.1.1	Policy on the use of cryptographic controls
		A.10.1.2	Key management Control
A.11.1	SECURE AREAS	A.11.1.1	Physical security perimeter
		A.11.1.2	Physical entry controls
		A.11.1.3	Securing offices, rooms and facilities
		A.11.1.4	Protecting against external and environmental threats
		A.11.1.5	Working in secure areas
		A.11.1.6	Delivery and loading areas
A.11.2	EQUIPMENT	A.11.2.1	Equipment siting and protection
		A.11.2.2	Supporting utilities
		A.11.2.3	Cabling security
		A.11.2.4	Equipment maintenance
		A.11.2.5	Removal of assets
		A.11.2.6	Security of equipment and assets off-premises
		A.11.2.7	Secure disposal or reuse of equipment
		A.11.2.8	Unattended user equipment
		A.11.2.9	Clear desk and clear screen policy
A.12.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES	A.12.1.1	Documented operating procedures
		A.12.1.2	Change management
		A.12.1.3	Capacity management
		A.12.1.4	Separation of development, testing and operational environments
A.12.2	PROTECTION FROM MALWARE	A.12.2.1	Controls against malware
A.12.3	BACKUP	A.12.3.1	Information backup
A.12.4	LOGGING AND MONITORING	A.12.4.1	Event logging
		A.12.4.2	Protection of log information
		A.12.4.3	Administrator and operator logs
		A.12.4.4	Clock synchronisation
A.12.5	CONTROL OF OPERATIONAL SOFTWARE	A.12.5.1	Installation of software on operational systems
A.12.6	TECHNICAL VULNERABILITY MANAGEMENT	A.12.6.1	Management of technical vulnerabilities
		A.12.6.2	Restrictions on software installation
A.12.7	INFORMATION SYSTEMS AUDIT CONSIDERATIONS	A.12.7.1	Information systems audit controls

Control Domain Code	Control Domain Name	Control Code	Control Name
A.13.1	NETWORK SECURITY MANAGEMENT	A.13.1.1	Network controls
		A.13.1.2	Security of network services
		A.13.1.3	Segregation in networks
A.13.2	INFORMATION TRANSFER	A.13.2.1	Information transfer policies and procedures
		A.13.2.2	Agreements on information transfer
		A.13.2.3	Electronic messaging
		A.13.2.4	Confidentiality or nondisclosure agreements
A.14.1	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	A.14.1.1	Information security requirements analysis and specification
		A.14.1.2	Securing application services on public networks
		A.14.1.3	Protecting application services transactions
A.14.2	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	A.14.2.1	Secure development policy
		A.14.2.2	System change control procedures
		A.14.2.3	Technical review of applications after operating platform changes
		A.14.2.4	Restrictions on changes to software packages
		A.14.2.5	Secure system engineering principles
		A.14.2.6	Secure development environment
		A.14.2.7	Outsourced development
		A.14.2.8	System security testing
		A.14.2.9	System acceptance testing
A.14.3	TEST DATA	A.14.3.1	Protection of test data
A.15.1	INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS	A.15.1.1	Information security policy for supplier relationships
		A.15.1.2	Addressing security within supplier agreements
		A.15.1.3	Information and communication technology supply chain
A.15.2	SUPPLIER SERVICE DELIVERY MANAGEMENT	A.15.2.1	Monitoring and review of supplier services
		A.15.2.2	Managing changes to supplier services
A.16.1	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	A.16.1.1	Responsibilities and procedures
		A.16.1.2	Reporting information security events
		A.16.1.3	Reporting information security weaknesses
		A.16.1.4	Assessment of and decision on information security events
		A.16.1.5	Response to information security incidents
		A.16.1.6	Learning from information security incidents
		A.16.1.7	Collection of evidence
A.17.1	INFORMATION SECURITY CONTINUITY	A.17.1.1	Planning information security continuity
		A.17.1.2	Implementing information security continuity
		A.17.1.3	Verify, review and evaluate information security continuity
A.17.2	REDUNDANCIES	A.17.2.1	Availability of information processing facilities

Control Domain Code	Control Domain Name	Control Code	Control Name
A.18.1	COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS	A.18.1.1	Identification of applicable legislation and contractual requirements
		A.18.1.2	Intellectual property rights
		A.18.1.3	Protection of records
		A.18.1.4	Privacy and protection of personally identifiable information
		A.18.1.5	Regulation of cryptographic controls
A.18.2	INFORMATION SECURITY REVIEWS	A.18.2.1	Independent review of information security
		A.18.2.2	Compliance with security policies and standards
		A.18.2.3	Technical compliance review
ANSSI.1.1	CONFIGURATION	ANSSI.1.1.1	System services
		ANSSI.1.1.2	Peripheral and removable equipment
ANSSI.1.2	MAPPING	ANSSI.1.2.1	Information Systems Mapping
ANSSI.1.3	LOGS MONITORING AND CORRELATION	ANSSI.1.3.1	Logs correlation and analysis
ANSSI.1.4	PARTITIONING	ANSSI.1.4.1	Partitioning of the system in physical sub-systems
		ANSSI.1.4.2	Partitioning of the system in logical sub-systems
ANSSI.1.5	FILTERING	ANSSI.1.5.1	Data filtering
ICAO.1.1	AIRPORT SECURITY - SECURITY RESTRICTED AREA ACCESS	ICAO.1.1.1	Access to airside area
		ICAO.1.1.2	Access to security restricted area
		ICAO.1.1.3	Security area establishment
ICAO.1.2	AIRPORT SECURITY - SECURITY CONTROL	ICAO.1.2.1	Screening of persons and goods
		ICAO.1.2.2	Examination of vehicles
ICAO.1.3	AIRPORT SECURITY - SURVEILLANCE	ICAO.1.3.1	Surveillance, patrols and other physical controls
ICAO.1.4	AIRPORT SECURITY - DEMARCATED AREAS OF AIRPORTS	ICAO.1.4.1	Aircraft parking areas
ICAO.1.5	AIRPORT SECURITY - AIRCRAFT SECURITY	ICAO.1.5.1	Aircraft security check
ICAO.1.6	AIRPORT SECURITY - AIRPORT SUPPLIES	ICAO.1.6.1	Airport supplies
ICAO.1.7	AIRPORT SECURITY - SECURITY ORGANIZATION	ICAO.1.7.1	In flight security measures - flight crew compartment
		ICAO.1.7.2	In flight security measures - disruptive passengers
		ICAO.1.7.3	In flight security measures - unlawful interference training
		ICAO.1.7.4	In flight security measures - general weapons regulations
		ICAO.1.7.5	In flight security measures - security officer weapons regulations

Control Domain Code	Control Domain Name	Control Code	Control Name
		ICAO.1.7.6	Training and recruitment of the staff
		ICAO.1.7.7	Security equipment
		ICAO.1.7.8	Personnel training versus cyber threats
ICAO.2.1	CARGO SECURITY - CARGO AND MAIL	ICAO.2.1.1	Security controls for cargo and mail
		ICAO.2.1.2	Protection of cargo and mail
		ICAO.2.1.3	Air carrier mail/materials security check
		ICAO.2.1.4	High risk cargo
ICAO.3.1	BAGGAGE AND PASSENGER SECURITY - PASSENGERS AND CABIN BAGGAGE	ICAO.3.1.1	Screening of passengers and cabin baggage
		ICAO.3.1.2	Protection of passengers and cabin baggage
		ICAO.3.1.3	Departing and arriving passengers separated
		ICAO.3.1.4	Potentially disruptive passengers
		ICAO.3.1.5	Passengers subjected to proceedings
		ICAO.3.1.6	Weapons carriage
ICAO.3.2	BAGGAGE AND PASSENGER SECURITY - HOLD BAGGAGE	ICAO.3.2.1	Screening of hold baggage
		ICAO.3.2.2	Protection of hold baggage
		ICAO.3.2.3	Baggage reconciliation
ICAO.4.1	GOODS IN FLIGHT SECURITY MEASURES - GOODS IN FLIGHT	ICAO.4.1.1	Goods in-flight security check