SATIE

Security of Air Transport Infrastructures of Europe

D7.7 – Specification of a holistic security management cycle

Deliverable Number	D7.7
Author(s)	KEMEA, AIA, SEA, ZAG, DLR, FHG, Teclib, ALS, ACS, NIS, SAT
Due/delivered Date	M19/2020-11-30
Reviewed by	DLR, KEMEA, ACS
Dissemination Level	PU
Version of template	1.07

Start Date of Project: 2019-05-01

Duration: 27 months

Grant agreement: 832969

DISCLAIMER

Although the SATIE consortium members endeavour to deliver appropriate quality to the work in question, no guarantee can be given on the correctness or completeness of the content of this document and neither the European Commission, nor the SATIE consortium members are responsible or may be held accountable for inaccuracies or omissions or any direct, indirect, special, consequential or other losses or damages of any kind arising out of the reliance upon the content of this work.

The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. All intellectual property rights are owned by the SATIE consortium members and are protected by the applicable laws. Except where otherwise specified, all document contents are: "©SATIE Project - All rights reserved". Reproduction is not authorised without prior written agreement.

Document contributors

No.	Name	Role (content contributor / reviewer / other)
1	Eftichia Georgiou, KEMEA	Content Contributor
2	Vasiliki Mantzana, KEMEA	Content Contributor
3	Ioannis Chasiotis, KEMEA	Content Contributor
4	Ilias Gkotsis, KEMEA	Content Contributor
5	David Lancelin, ACS	Reviewer
6	Corinna Köpke, FHG	Content Contributor
7	Katja Faist, FHG	Content Contributor
8	Nikolaos Papagiannopoulos, AIA	Content Contributor
9	Tim Stelkens-Kobsch, DLR	Content Contributor
10	Meilin Schaper, DLR	Reviewer
11	François Déchelle, Teclib	Content Contributor
12	Elena Branchini, SEA	Content Contributor
13	Thomas Oudin, ACS	Content Contributor
14	Leonidas Perlepes, SAT	Content Contributor
15	Sven Hrastnik, ZAG	Content Contributor
16	Kelly Burke, NIS	Content Contributor
17	Matteo Mangini, NIS	Content Contributor
18	Éric Hervé, ALS	Content Contributor

Document revisions

Revision	Date	Comment	Author
V0.1	2020-11-16	Final draft for public version based on D2.4	Eftichia Georgiou
V0.1	2020-11-30	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2020-11-30	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

The deliverable documents the results of T2.3: Harmonisation of approaches to achieve a holistic security management-cycle and presents an overview of i) the phases of the crisis management cycle (preparedness, response, recovery and mitigation) in the context of airports and the general practices applied ii) the key airport stakeholders and operation centres involved in airports iii) a refined list of rules and policies as well as safety and security procedures that best suit the needs of the projects' activities and systems of interest (intentionally not included in this report) iv) the main operations executed by the Airport Operation Centres of the participating airports and the various activities coordinated by these centres (intentionally not included in this report), v) the holistic cyber and physical crisis management cycle including the stakeholders and the relevant processes and finally the SATIE holistic crisis management approach.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
AAIASB	Air Accident Investigation and Aviation Safety Board
ABC	Automated Border Control
ABoD	Airport's Board of Directors
AC	Access Control
ACI	Airports Council International
ACRP	Airport Cooperative Research Program
ACS	Access Control System
ADO	Airport Duty Officer
ADS	Airside Duty Supervisor
AEP	Airport Emergency Plan
AFTN	Aeronautical Fixed Telecommunications Network
AIA	Athens International Airport S.A.
AI	Artificial Intelligence
ALS	ALSTEF AUTOMATION
AMI	Apron Monitoring and Inspection Unit
AMIC	Airfield Monitoring inspection coordinator
AOC/APOC	Airport's Operation Centre
AOCC	Airport Operations Control Centre
AODB	Airport Operations Database
ASOC	Airport Services Operations Centre
ATC / S	Air Traffic Control / Systems
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
BHS	Baggage Handling System
BMS	Building Management System
BSM	Baggage Source Message
CAA	Civil Aviation Authority
CAS	Crisis Alerting System
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives

Acronym	Definition
ACS	AIRBUS CYBERSECURITY SAS
CCTV	Closed-circuit television
CDM	Collaborative Decision Making
CERT	Computer Emergency Response Team
CFMU	Central Flow Management Unit
CI	Critical Infrastructures
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructures Protection
CIWIN	Critical Infrastructure Warning Information Network
CM	Crisis Management
CMC	Crisis Management Centre
CMT	Crisis Management Team
COP	Common Operating Picture
CSIRT	Computer Security Incident Response Team
DER	endpoint detection and remediation
DLR	DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV
DoS	Denial-of-Service
DPO	Data Protection Officer
EC	European Commission
ECI	Assets, systems or parts thereof located in EU member states, which are essential for vital societal functions [...] the disruption or destruction of which would have a significant impact on at least two EU member states
EDS	Explosive Detection System
EISAS	European Information Sharing and Alert System
EMA	Emergency Management Agencies
EMS	Emergency Medical Services
ENAC	Italian Civil Aviation Authority (Ente Nazionale per l'Aviazione Civile)
ENAV	Italian company owned by the Ministry of Economy and Finances
EOC	Emergency Operations Centre
EP3R	European Public Private Partnership for Resilience

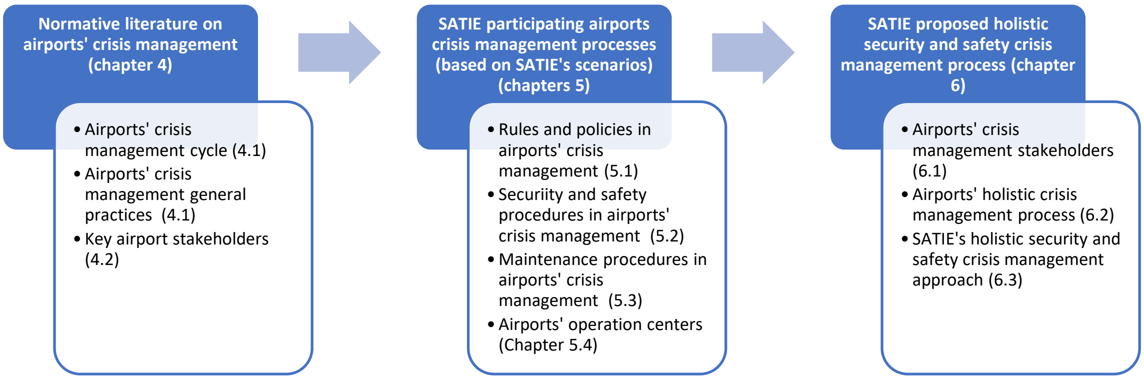
Acronym	Definition
EPCIP	European Programme on Critical Infrastructure Protection
FAA	Federal Aviation Administration
FD	Flight Data Duties
FDRA	Flight Data Resources allocation
FHG	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
FIDS	Flight Information Display Systems
FIS	Flight Information Service
GCC	Galileo Control Centre (GCC)
GDF	Guardia di Finanza (GdF) (Italian law enforcement agency)
GDPR	General Data Protection Regulation
GLPI	Gestionnaire Libre de Parc Informatique (en: Free IT Equipment Manager)
GRC	Governance, Risk and Compliance
GSCP	General Secretariat for Civil Protection
HCAA	Hellenic Civil Aviation Authority
HMI	Human Machine Interface
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICS	Industrial Control Systems
ICS	Incident Command System
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
ILM	Information Lifecycle Management
IOC	Indicator of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IS	Information System
IT	Information Technology
ITSM	IT Service Management
KEMEA	KENTRO MELETON ASFALEIAS
LEAs	Law Enforcement Agencies

Acronym	Definition
LoRa	Long Range
LoS	Level of Service
LS	Landside Supervisor
MAIS	Malpensa Airport Information System
MCS	Manual Coding Station
MITM	man-in-the-middle attack
ML	Machine Learning
MOC	Mission Operations Centre
MTBF	Mean Time Between Failure
MTTF	Mean Time to Failure
NGO	Non-governmental organization
NIMS	National Incident Management System
NIS	Network Integration and Solutions SRL (company)
NIS	Network and Information Security
NIS directives	Network and information systems directives
NIST	National Institute of Standards and Technology
NOC	Network Operations Centre
OP	Operational Phase
OSC	On Scene Commander
OSP	obligatory unless similar regulations are in place
PA	Public Announcement
PRM	Passengers with Reduced Mobility
PSIM	Physical Security Information Management
RA	Resources Allocation duties
RIS	Risk Integrated Service
RMS	Resource Management System
RFFS	Rescue and Fire Fighting Services
SA	Situational Awareness
SARPs	Standards and Recommended Practices
SAC	Sort Allocation Computer
SAT	SATWAYS

Acronym	Definition
SCADA	Supervisory Control and Data Acquisition
SDS	Security Duty Supervisor
SEA	SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA
SESAR	Single European Sky ATM Research
SIEM	Security Information and Event Management
SITA	Air transport communications and information technology (Company)
SMS-CB	SMS broadcast
SOC	Security Operation Centres
SOP	Standard Operating Procedures
STA	Scheduled Arrival Time
SWIM	System Wide Information Management
TETRA	Terrestrial Trunked Radio
TIP	Threat Intelligence Platforms
TMO	Ten Minutes Out
TOC	Threat Operations Centre
TOS	Terminal Operations Supervisor
UC	Unified Command and Control Centre
UEBA	User and Entity Behaviour Analytics
UFIS	Universal Flight Information
UTM	Unified Threat Management
VPN	Virtual Private Network
VuMS	Vulnerability Management System
ZAG	Zagreb airport - MEDUNARODNA ZRACNA LUKA ZAGREB DD

1 Introduction

The document outlines the results of the task T2.3: Harmonisation of approaches to achieve a holistic security management-cycle in the context of SATIE. In doing this, in chapter 4 the normative review of the phases of the crisis management cycle (preparedness, response, recovery and mitigation) in the context of airports as well as general practices applied, are presented. Moreover, the key airport stakeholders and operation centres involved in airports operations, as well as during the crisis management are analysed. Then, a refined list of rules and policies as well as safety and security procedures that best suit the needs of the projects' activities and systems of interest are presented in chapter 5. The presentation of the information is organised around the phases of the crisis management cycle. In addition, the main operations executed by the Airport's Operation Centre (AOC), the various activities coordinated by the AOC, the safety and security procedures and its role in case of an emergency are analysed in section 4.3 and 5.3. Finally, by combining information provided in chapters 4 and 5 a holistic cyber and physical crisis management cycle including the stakeholders and the relevant processes are proposed in sections 6.1 and 6.2. Finally, the SATIE holistic crisis management approach is presented in section 6.2.



Normative literature on airports' crisis management (chapter 4)

- Airports' crisis management cycle (4.1)
- Airports' crisis management general practices (4.1)
- Key airport stakeholders (4.2)

SATIE participating airports crisis management processes (based on SATIE's scenarios) (chapters 5)

- Rules and policies in airports' crisis management (5.1)
- Secuiity and safety procedures in airports' crisis management (5.2)
- Maintenance procedures in airports' crisis management (5.3)
- Airports' operation centers (Chapter 5.4)

SATIE proposed holistic security and safety crisis management process (chapter 6)

- Airports' crisis management stakeholders (6.1)
- Airports' holistic crisis management process (6.2)
- SATIE's holistic security and safety crisis management approach (6.3)

Figure 1.1: Document structure

For the needs of the specific deliverable D7.7, the input from the participating airports led to the establishment of a holistic security management cycle that comes along with harmonized processes and procedures for cyber and physical security and addresses the four phases of the crisis management cycle, namely: preparedness, response, recovery and mitigation. KEMEA with the support of partners provided descriptions of crisis management processes and profiles of stakeholders involved in these processes. The participating airports provided their strong experience in security operations management based on their daily activity as large European airports. DLR and NIS have supported the analysis of existing approaches and the harmonization of roles and procedures needed in a holistic security management cycle. FHG and Teclib provided insights about resilience strategies against systems deprecation and single nodes failure. ALS revised maintenance procedures on the Baggage Handling System (BHS). ACS provided information about cyber incident management in a SOC and SAT provided information about the crisis alerting system.

2 SATIE Overview

SATIE aims to build a security toolkit (see Figure 2.1) in order to protect critical air transport infrastructures against combined cyber-physical threats. This toolkit will rely on a complete set of semantic rules that will improve the interoperability between existing systems and enhanced security solutions, in order to ensure more efficient threat prevention, threat and anomaly detection, incident response and impact mitigation, across infrastructures, community and environment. Synchronously and relying on the security toolkit, SATIE will foster the implementation of an updated security management cycle within airports that will encompass security, safety, maintenance and information sharing processes. Over a 24-month time frame, the SATIE consortium will develop, test, validate and demonstrate in operational conditions 14 innovative elements which will optimise airport security. The consortium involves three large airports from three different countries and security forces to ensure that SATIE security toolkit is scalable and adaptable to the operational needs, and compliant with the emerging regulations and standards at national and European level. Different threat scenarios combining cyber and physical threats against airports will be defined and integrated in a simulation platform to validate the efficiency of the toolkit. In addition to simulations, different possible threat demonstrations will be conducted at three different airports in distinct locations across Europe. At the end of the project, the results will be disseminated and exploited in order to ensure a better airport security and improve passenger security and safety.

Taking into consideration current regulations, standards and daily challenges faced by the airports, SATIE partners have identified several security gaps that need to be addressed during the project. The following is a non-exhaustive list of the identified gaps:

- Usual risk assessment methods often lead to underestimate complex cyber-physical attacks because of their lack of predictability. They are prepared during months/years and they can destabilize large organizations, nations and unions.
- A clear mapping between airport assets and airport operations is missing (e.g. business processes). Cyber-physical detection rules and impact propagation models might be significantly improved with this knowledge.
- Command-and control systems (like the Baggage Handling System) are not sufficiently secured in the airports and there are a large number of unmanaged ICS, SCADA and IoT assets.
- Radio communication networks (e.g. Wi-Fi, LoRa) are insufficiently secured and IoT assets represent easy targets whereas they are increasingly used in the industrial and Information and Communication Technologies (ICT) systems of the airports.
- Air Traffic Management SWIM (System Wide Information Management) services are emerging, but they are still not secured and not traceable.
- Spamming and spoofing attacks on voice communication networks put airside/landside operations at risk.
- Baggage with lost tags raise breaches: the link between passenger and baggage could be better managed through an extended passenger identity and enhanced video monitoring with picture recognition of passengers' baggage.
- Anomaly detection on passenger data is still frequent in the airports and need to be improved.
- Correlation between physical and cyber security events is not easy to perform due to the lack of interoperability between physical and cyber security solutions (e.g. access control systems, incident detection systems, etc.).
- Forensics investigation tools are not specifically focused on multistep scenarios of threat combining cyber and physical security events that can be very distant in time.

- Lack of structured communication and harmonized procedures between the AOC, SOC, local authorities, first-responders and maintenance teams.
- Airports are considered as critical infrastructures and do not comply fully with NIS directives or/and GDPR law.
- Lack of cost-effective solutions for cyber-physical security whereas the budget on airports side is very limited to cover security requirements defined by national and European authorities.
- Beside the challenges to fill the aforementioned gaps, additional challenges are to integrate those functionalities together, and to update security policies in favour of a simplified change management.

A common awareness to security as a whole shall be raised, together with harmonized roles, responsibilities and procedures, ensuring improved prevention, detection, response, mitigation and recovery against physical and cyber security threats and attacks.

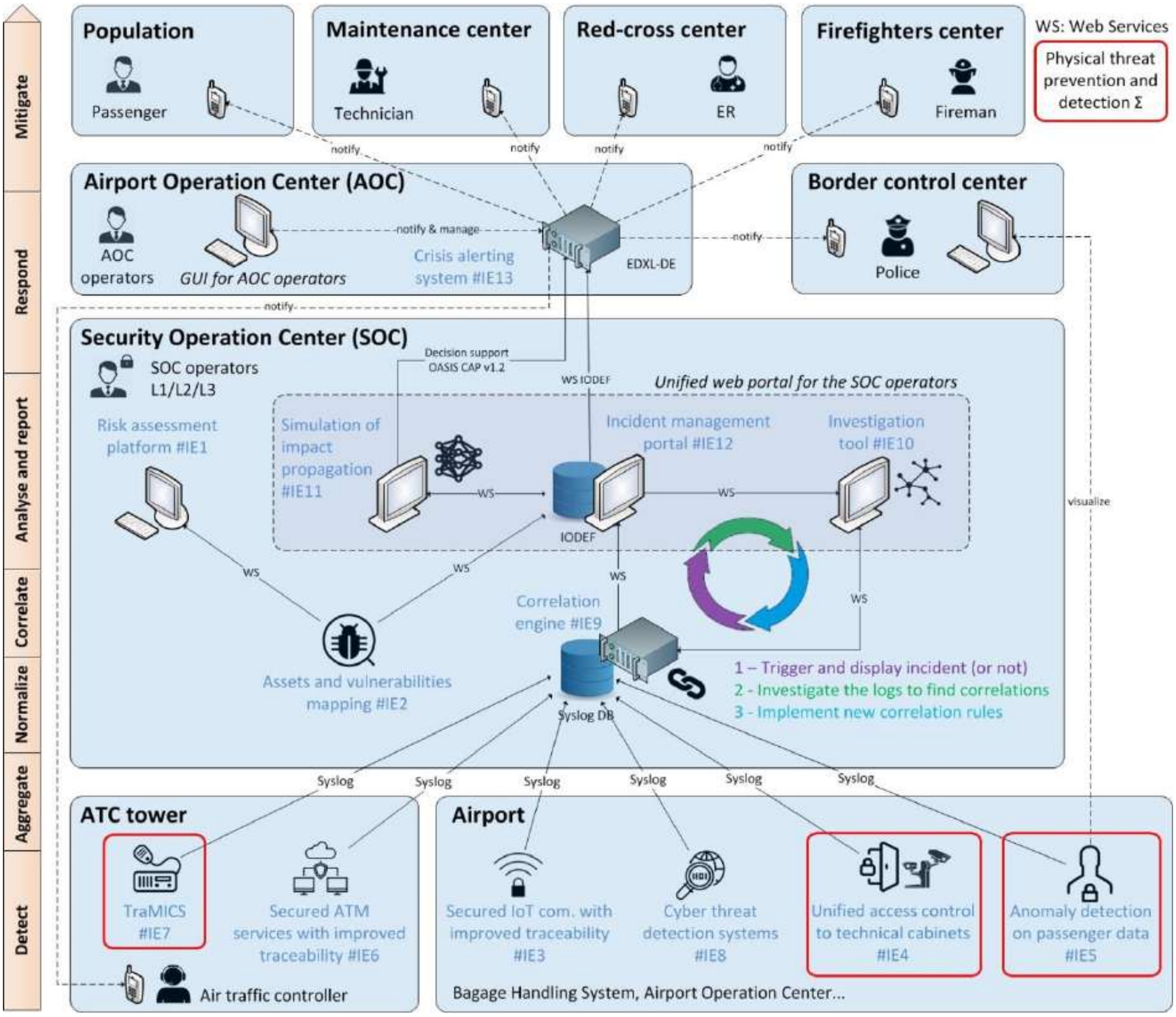

Mitigate
Respond
Analyse and report
Correlate
Normalize
Aggregate
Detect
Population
Passenger
Maintenance center
Technician
Red-cross center
ER
Firefighters center
Fireman
WS: Web Services
Physical threat prevention and detection Σ
notify
notify
notify
notify
Airport Operation Center (AOC)
AOC operators
GUI for AOC operators
notify & manage
Crisis alerting system #IE13
EDXL-DE
notify
Border control center
Police
notify
Security Operation Center (SOC)
SOC operators L1/L2/L3
Decision support OASIS CAP v1.2
WS IODEF
Unified web portal for the SOC operators
Risk assessment platform #IE1
Simulation of impact propagation #IE11
Incident management portal #IE12
Investigation tool #IE10
WS
WS
IODEF
visualize
WS
WS
WS
WS
Correlation engine #IE9
Assets and vulnerabilities mapping #IE2
1 – Trigger and display incident (or not)
2 - Investigate the logs to find correlations
3 - Implement new correlation rules
Syslog DB
Syslog
Syslog
Syslog
Syslog
Syslog
Syslog
ATC tower
TraMICS #IE7
Secured ATM services with improved traceability #IE6
Air traffic controller
Airport
Secured IoT com. with improved traceability #IE3
Cyber threat detection systems #IE8
Unified access control to technical cabinets #IE4
Anomaly detection on passenger data #IE5
Bagage Handling System, Airport Operation Center...

Figure 2.1: SATIE's overall concept and architecture

3 Critical Infrastructures Protection (CIP)

Europe has a long-standing history of approaches to improve Critical Infrastructure (CI) protection. Past terrorist attacks fostered the development and adoption of the European Programme on Critical Infrastructure Protection (EPCIP). The EPCIP provides systematic, network-based guidelines for member states to identify CI assets (1). The EPCIP comprises the following pillars (2): (a) means for its implementation (e.g., EPCIP action plan, CIWIN), (b) support for member states concerning National CIP, (c) contingency planning, (d) external dimension (exchange of information with non-EU countries), (e) EU security research program on "prevention, preparedness and consequence management of terrorism and other security related risks" and (f) financial measures.

The Directive 2008/114/EC functions as the main instrument of the EPCIP. Firstly, it provides definitions of CIs and ECIs. According to the Directive, ECIs are: "Assets, systems or parts thereof located in EU member states, which are essential for vital societal functions [...] the disruption or destruction of which would have a significant impact on at least two EU member states" (3). The directive provides concrete support for three phases of EPCIP. The phase of identification includes specific criteria to identify CIs: (a) sectoral criteria (b) CI definition, (c) transboundary elements and (d) cross-cutting criteria. The phase of designation includes all steps to negotiate and to decide on the criticality of any specific infrastructure: (a) notification of affected member states, (b) bilateral discussions and agreements and (c) final decision by the 'hosting country'. Finally, it provides two instruments that really contribute to the protection of infrastructures: (a) OSP (obligatory unless similar regulations are in place) and (b) liaison officer as contact point between the ECI owner/operator and relevant member state authorities.

Critical Infrastructures are complex, and they are turning into cyber-physical infrastructures because Information and Communication Technologies (ICT) are important in the context of infrastructure management. Today, most of organizations are susceptible to cyber threats because they are increasingly exposed to the internet and to the external world. Technological trends like Internet of Things (IoT), Industry 4.0 are driving this augmented connectivity. Nowadays, most Critical Infrastructures are controlled by Industrial Control Systems (ICS) that need to be frequently updated during maintenance campaigns. Since the beginning of the 21st century, Critical Infrastructures have faced multiple cyber and physical attacks.

The European Commission (4) recognises that an integrated EU approach to enhance the security and resilience of Critical Information Infrastructures (CIIs) would enhance national programmes and improve the existing bilateral and multilateral cooperation schemes between Member States. Public policy discussions in the aftermath of events, such as the recent large-scale cyber-attacks on Estonia, Lithuania and Georgia suggest that the effects of similar attacks can be limited by preventive measures and by well-coordinated action during the actual crisis. Based on the same report a multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities. The EC in 2009 included an action plan based on five pillars, involving the Member States and the private sector, in order to respond to current challenges and build a framework for enhancing network and information security. The major achievements are summarised below:

(1) Preparedness and prevention: to ensure preparedness at all levels:
- Strategic pan European Public Private Partnership for Resilience (EP3R).
- European Forum for information sharing between Member States.
- Baseline Capabilities of National/Governmental CERTs.
- Cross-country co-operation between National/Gov CERTs.

(2) Detection and response: to provide adequate early warning mechanisms:

- European Information Sharing and Alert System (EISAS).

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII:
- National Contingency Plans and Exercises.
- Pan-European exercises on large-scale network security incidents.
- Reinforced cooperation between National / Governmental CERTs.

(4) International cooperation: to promote EU priorities internationally:
- European and global priorities, principles and guidelines on long term Internet resilience and stability.

(5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures.

The Council Conclusion on CIIP issued in May 2011, taking stock of the results achieved since the adoption of the CIIP action plan in 2009, was launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures. The European Commission has also published a European Cyber Security Strategy and proposed a directive on Network and Information Security (NIS).

In the context of airports, the International Civil Aviation Organization (ICAO) works with Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies. The regulations and policies suggested by ICAO are adopted by ICAO Member States to ensure that their local civil aviation operations and regulations conform to the suggested norms, in order to ensure safety and security. Currently, EC regulation 300/2008 of the European Parliament and of the Council establishes common rules in the European Union to protect civil aviation against acts of unlawful interference. The regulation implements the EC regulation 1998/2015. The regulation's provisions apply to all airports, all operators that provide services at the airports, all entities located inside or outside airport premises providing services to airports. More details about the rules and policies are provided in Table 5.3: Physical rules and policies.

4 Crisis management cycle in the context of airports

In this chapter, the phases of the crisis management cycle in the context of airports are described and general practices applied are presented. Moreover, the key airport stakeholders and operation centres involved in airports operations, as well as during the crisis management are presented.

4.1 Crisis management cycle phases

EPCIP and Directive 114 focus on the sectors of Energy and Transport. As further analysed within, Air Transport is one of the infrastructures that need to be protected, due to its criticality for the society. Airports, being CIs that belong to this subsector, play a key role in people and goods transportation, as well as in regional, national and international trade. Along the years, more and more people use airplanes as a frequent mean of transport. As stated in SESAR project PJ04 (5) 7.2 billion air travellers are expected by the International Air Transport Association (IATA) to travel in 2035, while this number in 2016 was cut close to half (3.8 billion). A 3.7% annual compound average growth rate is used to make this forecast. In 2017, air passengers in the European Union reached 1.043 billion, by 39% from 2009 and up by 7% compared to 2016.

They are one of the Critical Infrastructures where federal responsibility for overseeing and controlling air traffic operations intersects with local governments that own and operate most airports. Airports incorporate in their agenda passenger comfort, cost-efficiency, environmental protection and policies for corporate and social responsibility. They adopt policies that promote efficient collaboration among stakeholders (shareholders, air travellers, airlines, businesses, clients, business associates, local community and employees) and create a responsible sustainability plan and contemporary activities towards public safety, provided services, company employees and businesses operating within the airport's premises. More passengers in aviation should lead to better performance but this also demands better security measures and control procedures in order to safeguard travellers.

It has been reported that airports are exposed to various physical threats that can be classified as aviation and non-aviation related, including terrorism, Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE), technological accidents, natural disasters, etc. (6). In addition to this, cyber-attacks to airport operations are emerging especially with the increasing use of Information Systems (IS), such as electronic tags for baggage handling and tracking, remote check-in, smart boarding gates, faster and more reliable security screening technologies and biometric border controls etc. Any physical or cyber threat that causes loss of infrastructure or massive patient surge, such as natural disasters, terrorist acts, or chemical, biological, radiological, nuclear, or explosive hazards, denial-of-service attack (DoS attack), man-in-the-middle attack (MITM), etc. could affect airports' services provision and could cause overwhelming pressure to the affected systems.

It appears that it is fundamental for every airport to remain resilient, maintain the level of provided services, and be able to scale up its service delivery in any given emergency. Depending on the type of attack, airports aim to increase their capacity in order to respond effectively. Airport capacity, operations management and flight scheduling are vital elements for ensuring airports resilience. Among the consequences of the mismatch between the demand and the available capacity are the congestion in air and airport operations, the increase in costs and the decrease of safety levels at airports. In the case of man-made disasters, such as bio-terror attacks or chemical release events the main aim of an airport is to minimize the number of deaths and the proper decontamination of victims in order to prevent other people in and out of the airport getting infected (7). Based on literature findings a multidisciplinary approach among emergency medical services and airport authorities should be in place. Additionally, exhaustive safety and security plans, detection equipment and personal protective equipment for the first responders are among the minimum requirements in order to face such threats.

The management of a crisis does not start when the crisis occurs. The planning and coordination for response to any type of incident must be performed well in advance of an actual event. Crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises" (8). The full cycle of crisis management can be described in four phases: Preparedness, Response, Recovery, and Mitigation (Figure 4.1).

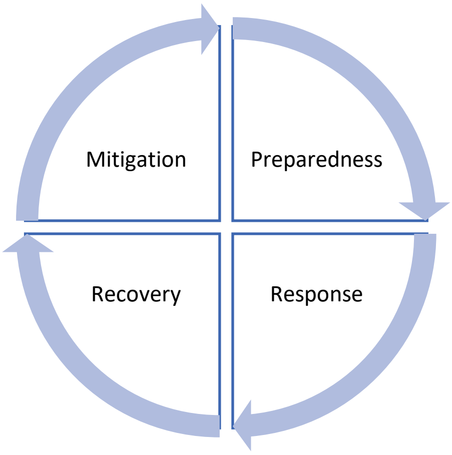


Figure 4.1: Crisis management

The concept of the cycle implies an ongoing process which tries to eliminate disruptions, to provide immediate assistance to affected ontologies, to reduce disaster losses and to improve the conditions of the affected communities. Usually, the crisis management cycle is triggered by an event and begins with the response to that event. As the main aim is to respond to the specific threat, crisis management programs often prioritize the preparedness and response phases, leaving limited resources to address recovery and mitigation. A systems approach to crisis management suggests a different understanding of the crisis cycle that balances resources among the four phases.

The crisis management is an exhaustive and extensive procedure that requires the integration and cooperation of multiple stakeholders (9) (10). Stakeholder management is considered as a crucial factor in all phases of crisis management as their actions can increase the public awareness, reduce the disaster consequences and enhance the mitigation actions. To that end, mutual aid agreements, clear communication pathways and trainings among stakeholders should be in place (11) (12). The main categories of stakeholders involved in crisis management planning are among others the following: host governments, military, local enterprises, regional aid agencies and international actors such as the larger aid agencies, extra-regional NGOs and logistics service providers.

Research is necessary to solve common operating problems and to facilitate the crisis management, to suggest and promote appropriate new technologies from other industries, and to bring innovations into the airport industry. The aviation industry needs to overcome the legacy processes and the old technology that keep them stuck. Latest technological developments such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain etc. create opportunities never seen before. Yet frameworks should foster the development with guidelines and pro-active measures to address liability, safety, security and privacy of these new technologies. The Airport Cooperative Research Program (ACRP) serves as one of the principal means by which the airport industry can develop innovative near-term solutions to meet demands placed on it. The ACRP undertakes research and other technical activities in a variety of airport subject areas, including design, construction, maintenance, operations, safety, security, policy, planning, human resources, and administration. The ACRP provides a forum where airport operators can cooperatively address common operational problems (13).

The four phases of crisis management in the context of airports are analysed in the following paragraphs.

4.1.1 Preparedness in the context of airports

Several events, starting from the world's first terrorist attack while in flight (Cubana Flight 455 on October 6, 1976) and the September 11 attacks, which are the most widely recognized terrorist attacks in recent times involving air travel, changed aviation and airport procedures deeply in terms of security techniques and methods used in an attempt to protect passengers, staff, aircraft and airport property from accidental/malicious harm, crime and other threats.

The aim of the preparedness phase is to prepare organisations and develop general capabilities that will enable them to deliver an appropriate response in any crisis and recover quickly after it. Preparedness refers to activities, plans, programs, and systems developed before crisis that will enhance capabilities of individuals, businesses, communities and governments to support the response to and recovery from future disasters.

During the last decades, the all-hazards concept of emergency preparedness has penetrated first the emergency management community, then the airport community. A plethora of surveys conducted in Europe and US around the concepts of prevention and preparedness, which are the most researched crisis management cycle stages with over 15,000 papers each (14), (15), (16) , emphasize the need for sound structural, organizational, policy, operational, and defensive relationships between airports and Emergency Management Agencies (EMA) in order to ensure community preparedness and the protection and promotion of both airport operations and business continuity. Airport managers have a deep understanding and appreciation that the benefits of cooperation with EMAs include efficiency of communications, leveraging personal relationships, mutual trust and mutual respect, rapid response as well as interoperability and interchangeability of skills and equipment. All these characteristics are essential to airport preparedness and can enhance airports' utility when communities face the unexpected.

In the context of physical emergency preparedness airports should assess their facilities and resources as described below (17):

- **Personnel.** Number of people trained to respond to emergencies at the airport and number of people highly familiarised with the airport's layout and operations. A 24-hour contact list should be in place. What should happen if the airport manager is not available? Who can be designated the point of contact during an emergency in his or her absence?
- **Equipment.** Type of emergency equipment needed and places to be stored. Airport staff members and emergency responders should know where this type of equipment is stored. Emergency response vehicles should be equipped with the appropriate communication radios.
- **Facilities.** A detailed drawing of the airport should be included in the emergency plan. Runway sizes, taxiways, ramps, buildings, access roadways, fence lines should be described. Additionally, critical sources of power, emergency generators, and water (hydrants) need to be located for quick access.
- **Terrain.** Understanding how easily areas off the end of the runways and in remote airport areas can be accessed. Assure that access roads are in good shape enabling rescue teams do their job.
- **Accessibility.** Calculate the distances and response times for responding agencies to the airport. Define the features that could affect the airport accessibility.

- **Communications**. Communication is one of the biggest barriers to effective emergency response. Define effective communication factors, such as frequencies used by the responding agencies, airfield communication characteristics, existence of incident command vehicles capable of coordinating multiple frequencies, etc.
- **Tabletop review.** The goal is to improve the emergency and security plans**.** All agencies involved in a potential emergency response to the airport should be invited to participate in an annual tabletop review.
- **Conducting a live exercise.** The FAA (Federal Aviation Administration) requires airports serving commercial airlines to conduct a live exercise drill of the emergency plan once every 36 months.
- **Developing an airport security plan.** A security plan can be helpful in planning for events that are not emergencies but still pose security threats to the airport.
- **National incident management system.** The system suggests planning guidelines and provides references for additional training and informational resources.

In the context of cybersecurity attacks, sensitive or confidential information may be leaked, or malware may be installed for activation later. It is of paramount importance for airports to detect attacks that occur as quickly as possible. The primary activities established by the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity are from one hand the identification of the critical assets (hardware and software) as well as data flows within the organization and from the other the implementation of countermeasures in a prioritized manner in order to protect their systems, data and infrastructure (18). Following are some practices that can help airports to be better prepared to identify cyber-attacks:

- **Risk assessment.** IT and facility managers should identify threats and risks that may impact airport data and systems. They should also be able to identify the motives of an attack (e.g. whether it is to obtain sensitive information, to disrupt operations, etc.) in order to prioritize countermeasures for their organisation.
- **Vulnerability assessment and estimation of impact**. This process should summarize the threats to which airport data and systems are exposed, as well as the impact that a successful attack may have on data and systems. The assessment of cybersecurity risks to critical infrastructure should consider the impact to the airport and National Airspace System operations, the number of affected users and stakeholders, loss of data, reputation and the public concern.
- **Maintenance of an updated inventory of assets.** IT systems and ICS, as well as the data stored or processed by these systems, are usually targets of cyber-attacks. Maintaining a detailed configuration management database will make protection and detection effective. The database should include information such as the criticality of systems/assets to airport operations, the vendors, software versions, patches, and updates. Additionally, the information in the inventory should be frequently updated as existing systems are reconfigured and new systems are installed.
- **Estimation of the likelihood of specific cyber-attacks.** In some cases, understanding the channels/avenues an attacker might use can help in assessing the likelihood of an attack.
- **Update the systems regularly.** Ensure that patches and updates to systems, should be applied, as they are made available by vendors.
- **Training.** Guidelines in the form of training material regarding the implementation of countermeasures should be distributed to airport personnel based on their role. Staff, consultants, and vendors should be continuously trained.

4.1.2 Response in the context of airports

Response requires a set of actions taken to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing events or disruptions and to recover to a normal situation (ISO 22300:2018). As undertaking and establishing an incident response effectively is complex, substantial planning and resources are required.

Airports should use different measures to detect an incident, including the implementation of intrusion detection systems, the logging infringement on airport infrastructure and the daily monitoring of security activities. When an attack is detected, steps should be followed to minimize the impact. These measures aim at analysing alerts, follow-up response procedures and form a crisis management cell as required by the severity of incidents. More specifically, reports of anomalous activity of systems, suspicious human activity and data breaches should be promptly communicated to the individuals responsible for security at the airport. These reports may come through help desk personnel, managers or security personnel. In addition, alerts of anomalous activity, attempted or unusual access requests, suspicious network traffic or other events that may indicate that an attack has occurred should be provided to designated personnel. Moreover, the impact of the reported activities should be determined and monitored quickly using information recorded in the inventory and collected from the vulnerability assessments.

Finally, if an issue is detected, those responsible for security at the airport should take the appropriate actions, based on a pre-defined response plan. A response plan is required, as it supports reporting of security breaches and compliance with security rules and allows organizations to identify, minimize the damage, and reduce the cost of a physical or cyber-attack. The incident response plan should: (a) provide a roadmap for implementing the incident response, (b) support the accurate documentation of events, (c) identify contributing factors that led to the incident and steps that should be taken to prevent the recurrence of a similar incident, (d) be distributed to internal and external stakeholders, as deemed necessary and (e) be frequently tested, evaluated and reviewed, as part of the preparedness and mitigation phases. In addition, the evacuation and patient transfer plans/processes which might be needed to be activated during the response phase, depending on the incident's type should be pre-defined. Response activities can be concurrent, and all should be subject to review and should adhere to the airport's policy and procedures. Since time is of the essence during a response, individuals who fulfil the roles required during a response should already be aware of and trained on these plans and processes, during the preparedness phase described in the above section. External resources should be considered and perhaps already under contract to assist in a response. Often such external resources have specialized training, experiences and resources needed to effectively respond and recover. In addition, airports should consider the coordination and sharing of information with internal and external stakeholders, including external service providers, organizations and media.

4.1.3 Recovery in the context of airports

When a crisis occurs, organizations must be able to carry on with their tasks during the crisis while simultaneously planning for how they will recover from the damage the crisis caused. Steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis (19). There are two main tasks in the recovery phase. During the first task, infrastructure should be examined, and repairs should be carried out to restore water, power, communication, and other physical and cyber utilities. Apart from the physical/cyber rebuilding or replacement of infrastructure that might be necessary, the organization should support investigations by police or relative regulatory authorities. The second task includes returning to normal functions and addressing future disasters. The recovery activities to be followed should be reflected in a response and recovery plan, such as business continuity/continuity of operations plans.

The following list outlines the best practices during recovery after physical or cyber crisis, emergency or disaster, as have been cited by participating airports in the relevant survey (20), as follows:

- **Recovery plan:** The most effective practice is to have a recovery plan accompanying each response plan. Recovery plans can involve all hazards or can be dedicated to separate hazards. Stakeholders as already mentioned in the preparedness section should be involved in this phase.

This step encompasses planning, training, preparing facilities and equipment, in order to ensure the availability of critical supplies and services as well as making financial and accounting arrangements.

- **Command and control**: The participating airports indicated that a Unified Command and Control Centre (UC) is of paramount importance. The UC consists of the ICS and NIMS responders, as well as representatives from stakeholders such as maintenance, IT, airlines, etc.
- **Comprehensive crisis communications:** Consistent and accurate communication of facts before, during and after the crisis eases effective recovery. Airports emphasize the necessity for effective and immediate communication with the public within their facilities during crisis. In general, airports understand that they cannot assume they can rely on cell phones, landlines, or the internet during an emergency or disaster. Additionally, some airports have technology systems specifically designed to drive Emergency Operations Centre (EOC) functions and/or share a common operating picture (COP) during events or emergencies.
- **Employee care:** Emergencies and accidents generally bring trauma, suffering and loss. Mental health trauma specialists should be available to employees to help them process the event in their own ways.
- **Customer care**: Most of the airports cited that airlines would meet the needs of the family and friends of victims.
- **Assessment, revision and validation of changes**: The airports review actions, outcomes and consequences to see what worked and what needs improvement, and incorporates the results into revised recovery plans, etc. The resulting plans and changed procedures are then typically tested using tabletop exercises, drills, and full-scale exercises (preparedness phase). The revised plans and procedures become the basis of updated training.

4.1.4 Impact mitigation in the context of airports

Mitigation refers to the process of reducing or eliminating future loss of life, property and injuries resulting from hazards through short and long-term activities. Mitigation strategies may range in scope and size. But no matter the size, effective mitigation activities can reduce vulnerability and exposure to risk from disasters. Airports risks that can limit the success of its safety and security programs should be periodically considered, as new risks should be identified, and the effectiveness of mitigation strategies will need to be evaluated.

In addition, an airport that has successfully been attacked should not return to normal operations as defined by the state of operations prior to the attack. New countermeasures, some of which may alter activities previously defined as “normal,” may need to be implemented. The attack should be carefully examined, and lessons learned should be extrapolated. These lessons should be applied to change policies, procedures and implement new or improved countermeasures. The efficiency and effectiveness of the response and recovery from an attack should also be reviewed to make improvements for the future. Metrics that attempt to quantify the cost of the attack in terms of operational downtime, loss of data and reputation, response and recovery should also be recorded to reassess the return on investment that additional measures may provide. Senior management should also reassess their willingness to tolerate attacks and make future investment decisions accordingly.

4.2 Key stakeholders in airports

Airports are variously accountable to many types of stakeholders, according to each airport’s ownership, mission and whether it is publicly or privately held. Based on the European Union Agency for Cybersecurity (ENISA) the key stakeholders that contribute to the functioning and operation of the smart airports, lie in two categories: Those that lie outside the direct boundaries and/or management of the airport and those that lie within the airport organisational boundary, as can been seen if the following Figure 4.2.

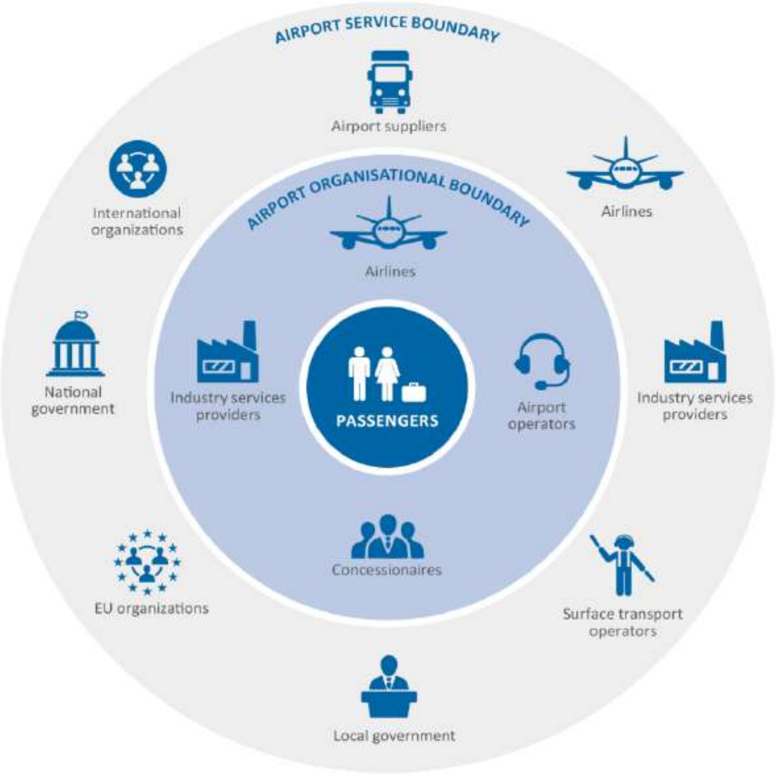


Figure 4.2: Smart Airports: Key Stakeholders (21)

The description of stakeholders as provided by ENISA is provided in the following Table 4.1.

Table 4.1: ENISA airports' stakeholders

Stakeholders	Description
Passengers	Customers of the airport, travel between the ground and air transportation modes or wait for a connection between two flights.
International /EU Organizations	They provide international standards, regulations and best practices. EUROCONTROL via the Central Flow Management Unit (CFMU) collects and distributes flight information among national air traffic controls to optimise Air Traffic Flow and Capacity Management (ATFCM) operations across Europe.
National Government	National Government participates in the airport system in two different ways: a) as an operator, focusing on air traffic control services, transportation systems, security (e.g. baggage handling and screening, and customs and immigration) b) as a regulator with regulations applying to airport infrastructure and service providers within airport systems.
Local Government	Local Government is usually responsible for the strategic direction of the airport (in terms of planning decisions) and for appointing airport management, depending on the ownership structure.
Industry/Third-Party	Service providers are private operators that offer services to air carriers and

Service Providers	general aviation users: 1) Air traffic management 2) fuel management 3) baggage handling and screening 4) cargo processing services 5) IT and Communication services 6) security services, etc.
Surface Transport Operators	Surface Transport Operators provide surface access to the airport and include rail services, buses, and the subway/underground, etc.
Airport Operators	An operator can manage either an airport or a group of airports e.g. Fraport.
Airlines	An airline is a company that provides air transport services for passengers and freight. Airlines utilise aircraft to supply these services and may form partnerships or alliances with other airlines for codeshare agreements. Generally, airline companies are recognised via an air operating certificate or license issued by a governmental aviation body.
Airport Suppliers	Airport suppliers have the airport itself as the end-customer. They include suppliers such as consulting services and equipment suppliers.
Concessionaires	Airport Concessionaires operate passenger services in terminal buildings and may include food and beverage services, retail and accommodation.

The interactions among the numerous stakeholders can be very complex. The IT systems that get involved in their interactions, based on the reports published by ENISA and ACRP (22), are often grouped into four conceptual categories and are depicted in a layered fashion (integration, application, networking and physical) as can been seen in the following Table 4.2.

Table 4.2: Conceptual categories of stakeholders' interactions (22; 21)

<table>
<tr><td><b>Airport Organizational Boundary</b>
shows the limit of what is controlled by airport management</td><td colspan="3"><b>INTEGRATION LAYER</b>
Systems Integration Layer - It allows sharing data and information among applications - Systems: Airport Operational Database (AODB), Geographic Information Display System, Message Broker, Systems manager</td><td><b>Airport Service Boundary</b>
Shows the airport supply chain and support services that lie outside direct management control of the airport</td></tr>
<tr><td colspan="5"><b>APPLICATION LAYER</b>
<b>Stakeholders Interaction</b></td></tr>
<tr><td rowspan="4"><b>Airside Systems</b>: Resource Management System, Surface Movement radar, Fuel Monitoring System <b>Landside systems:</b> Audio paging system, AVI, PARC, Roadway dynamic signage <b>Passenger processing systems:</b> Baggage sortation/RFID, MUFIDS <b>Business/Finance systems:</b> Asset Management system, Human resource management system, Email, Property management system <b>Safety/security systems:</b> Badging system, CCTV, Fire alarm, Police systems <b>Facility/maintenance systems:</b> Building</td><td>Best Practices Guidelines</td><td><b>International Organizations</b>
IATA
ICAO</td><td>International Regulations Chicago Convention</td><td rowspan="4">Aircraft Manufacturers
Airline Operations Centre
Central Flow Management Unit
ATM Information Management
Network Security Management Services
Equipment Suppliers
Floor Space Management
Consulting Services
Airport Administrative Duties
Building Maintenance
Legal and Financial Services
National Rail, Underground, Bus and Highways</td></tr>
<tr><td>ISMS/ISO Standards</td><td><b>EU Organizations</b>
European Commission
EASA
EUROCONTROL</td><td>European Data & Information Management and Distribution</td></tr>
<tr><td>Regulations</td><td><b>National Government</b>
National CAAs
Border Control</td><td>National Air Space Management</td></tr>
<tr><td>Planning, Governance</td><td><b>Local Government</b>
Transport Authorities
Planning Authorities
Local Communities</td><td>Planning, Procurement</td></tr>
</table>

management system, CMMS	Business Service Providers	**Industry** Third Party Providers Industry / Manufacturers Network Service Providers	ADS -B, Ground Stations, Beacons, GPS	
	Service Experience	**Passengers / Travelers**	Passenger Safety	
Airport IT Infrastructure (LAN, WAN, Wireless)	**NETWORKING LAYER**			VHF, VDML, Voice and Datalink ADS-B, ACARs (Flight Tracking)
Cable Infrastructure, Fiber Optic Infrastructure	**PHYSICAL LAYER**			Radar Beacons and Ground Stations

During a cyber or physical incident, different categories of stakeholders either internal or external might be fundamentally affected when an airport's routine operations are compromised and disrupted. For the needs of the crisis management analysis to follow in chapter 6, the definition of internal stakeholders refers to the individuals and parties belonging directly to the organisation/airport while externals stakeholders represent parties which are outside the organisation and affect or get affected by the organisation's activities (23). Typically, during a cyber or physical incident the following stakeholders are considered: i) internal (e.g. Data Protection Officer's (DPO), physical security manager/security personnel, IT security manager/security personnel, technical manager/ technical staff, security and safety teams, Crisis Management Team (CMT), etc.) and ii) external (e.g. interconnected/interdependent Critical Infrastructures and related organizations, Law Enforcement Agencies (LEAs), fire brigade, Emergency Medical Services (EMSs), civil protection authority, Air Accident Investigation and Aviation Safety Board (AAIASB), Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT) etc.). These stakeholders have different needs and requirements, trying to cooperate, respond and recover from the crisis. Airports' security stakeholders are individuals or organizations that may contribute to, be affected by, or get involved in issues related to security planning, response or recovery in any given emergency or posed threat.

4.3 Airport Operation Centres

Airport Operation Centres (AOCs) are tools to safeguard airports in their daily routine. The following sections provide an overview of the Operation Centres which are implemented in order to prevent attacks and enhance security. A description of the AOCs at the participating airports is provided in section 5.3.

Emergency Operations Centre (EOC): The EOC is a facility operating to manage disaster emergencies. It is the place where information management, allocation and coordination of resources, and recovery actions take place. EOC is a physical location but is not necessarily linked to IT security and could be formed in cases of natural disasters, civil and political unrest, and other events that could have an impact on operations, personnel and aircrafts. As the speed and accuracy of response is directly proportional to the timeliness and pertinence of the information obtained, gaining situational awareness is the priority of any effective EOC. Its focus rests on the preparedness, monitoring and response of potential emergency situations. It can be synonymous to crisis management centres, command and control centre, war room or other similar terms. An EOC constitutes a secure location where multi-agency response can be coordinated and representatives from all emergency response agencies coordinate their actions (24).

Mission Operations Centre (MOC): MOC comes together for a single planned event and then either would be disbanded or left with only core crew positions to maintain ongoing operations. **Air Traffic Control (ATC)** Centres are a type of permanent MOC and similar organizations may be seen in larger busy train stations. The most known MOCs focus on space operations and among others, there is the following: NASA's Christopher C. Kraft Jr. Mission Control Centre, the Galileo Control Centre (GCC) in the German Aerospace Centre (DLR).

Threat Operations Centre (TOC): Threats Operations Centres primarily focus on threats identification, characterization and attribution. In addition, they aim at information sharing and threat and situational awareness in order to analyse the threats and adopt mitigation strategies. Intelligence gathering and dissemination is the main aspect of their operation and is in direct connection with proper groups and teams that will perform counter threat strategies and actions.

Network Operations Centre (NOC): A NOC manages, control, monitor and maintain one or more networks. The main function is to maintain optimum network functionality and operations across various platforms, media and communication channels and to monitor the network status (internal or external). In addition, NOC capabilities include: application software installations, troubleshooting and updating, email management services, backup and storage management, network discovery and assessments, policy enforcement, firewall management, antivirus scanning and remediation, patch management and whitelisting, reporting and improvement recommendations.

Security Operations Centre (SOC): Technological assets are facing threats of cyber-attacks and data breaches, driving organisations to admit the need of securing their infrastructures and their technological tools, mechanisms and equipment. This security comes with a varying cost and budget constraints and competing priorities dictate moderate solutions and outsourcing. SOCs constitute a security need as they offer full security coverage of operations while they maintain acquisition and maintenance cost at a reasonable level. Bidou et al. mention that Security Operation Centre is a generic term describing part or all of a platform whose purpose is to provide detection and reaction services to security incidents (25). SOC monitors security posture of an organisation on an ongoing basis and is constituted of a security team (managers, security analysts and engineers) using various technological solutions in order to oversee security operations and to collect data via data flows, telemetry, packet capture and syslog to detect, identify, analyse, defend, investigate and report cybersecurity incidents. SOC architecture models can differ based on organisations' needs and preferences. Indicative SOC categories are: Dedicated or internal SOC (team within organisation), virtual SOC (team works remotely), global or command SOC (high-level group oversees smaller SOCs) and co-managed SOC (internal IT collaborating with outsourced vendor).

Typically, SOCs' **architecture**, where data is being aggregated and correlated from security feeds by a Security Information and Event Management (SIEM) system, incorporates a variety of systems such as vulnerability assessment solutions, security information, firewalls, breach detection solutions, Governance, Risk and Compliance (GRC) systems, application and database scanners, Intrusion Prevention Systems (IPS), User and Entity Behaviour Analytics (UEBA), Endpoint Detection and Remediation (EDR) and Tthreat Intelligence Platforms (TIP) .

Airport Operations Centre (AOC or APOC): An AOC incorporates all or a selection of the previous centres based on the operational needs of each airport. AOC constitutes an operational management structure that allows a common operational view and procedures and processes to relevant airport stakeholders in order to communicate, collaborate, coordinate and decide on the progress of airport operations. AOCs' purpose is to provide new means of supporting tools for arbitrated collaborative decision making. Fraport's Integrated Airport Operations report (26) highlights that terminal, airside or landside related airports' resources such as infrastructural, human and equipment can be supported and optimised with the use of the AOC and that the AOC, either as a distributed solution or as a centralized physical command and control room, can be seen as a core element of the Integrated Airport Operations system.

An AOC has several **characteristics** that include continuous data sharing amongst all partners, decision-making based on planning and simulation tools to support and include all airside and landside processes such as terminal and apron. Collected information allows collectively decision making towards smooth and proactive dialog among companies and services whilst remaining agilely in daily operations through fast information flow and adding value in crisis situations. Reports on airports' operations indicate the importance of airport key player's coordination in order to constantly have a clear and uniform overview of passenger flow, aircraft position on the tarmac and of the handling processes for departing, arriving and connecting baggage. The importance of information and data sharing among all airport stakeholders to increase operational efficiency is a fact. Technological equipment is also an important element in this process as it can improve data exchange and operational metrics regarding aircrafts, passengers and luggage. Successful AOC requires a clear role and undisruptive function agreed upon all stakeholders, (live) data sharing and reliable planning and simulation tools (27)**.**

Furthermore, capacity management can be enhanced by using AOC. Implementation is based on creating a shared and valued goal of all involved stakeholders, creation of a database with historical data, analysis of historical data for post-operations analysis, design of operational improvements and test of alternative scenarios and final implementation of tools, procedures and processes. Successful implementation of an AOC is performed with the contribution of involved stakeholders such as airlines, air traffic control providers, airport operator, ground handling agents and meteorological institutes. Also, crucial to AOCs' implementation and operations' efficiency are data on flight movements, data from the airport operator such as terminal processes and ground handling agents, airlines data such as turnaround processes and enriched data deriving from simulation and planning. Value will be added with the involvement of home carriers, baggage handling companies, security companies, companies who provide assistance to persons with reduced mobility, the police and various services of an airport including security, stand and gate allocation, airside inspection, passenger services and technical services. Those stakeholders should be eager to comply with a high intensity of data sharing to enable close collaboration among involved airport actors via Airport Collaborative Decision Making (28). The process of collaboration and data sharing requires overcoming technical challenges, such as standardisation and anonymization of data and secure transfer structures and channels, and a significant effort and investment in terms of personnel and actual implementation cost.

AOC can be implemented as a "centralized" or a "decentralized" system. The **centralized AOC** concerns an infrastructure (such as a room) where all relevant information is shared, merged and displayed to ensure upcoming decisions are effective. Information is simultaneously accessed from all AOC staff and stakeholders. This centralized AOC can be implemented as **Virtual AOC.** All relevant information such as actual traffic situation, planning, and ad hoc decisions are exchanged among the connected partners with the help of a network. This means that technical assistance is available to all stakeholders without structuring a physical AOC. The **decentralized AOC** can be seen as a centre with distinct functions which are established as separate data pools and connected with the monitoring, planning, and simulation tools. Connectivity between them is used only in extreme and urgent situations. This approach is more cost effective for an airport, but communication feasibilities are more complicated and there is no overview of all procedures simultaneously.

The following schema (Figure 4.3) indicates that the AOC should be an asset to strategic and pre-strategic airport management and that it linked with many vital compartments.

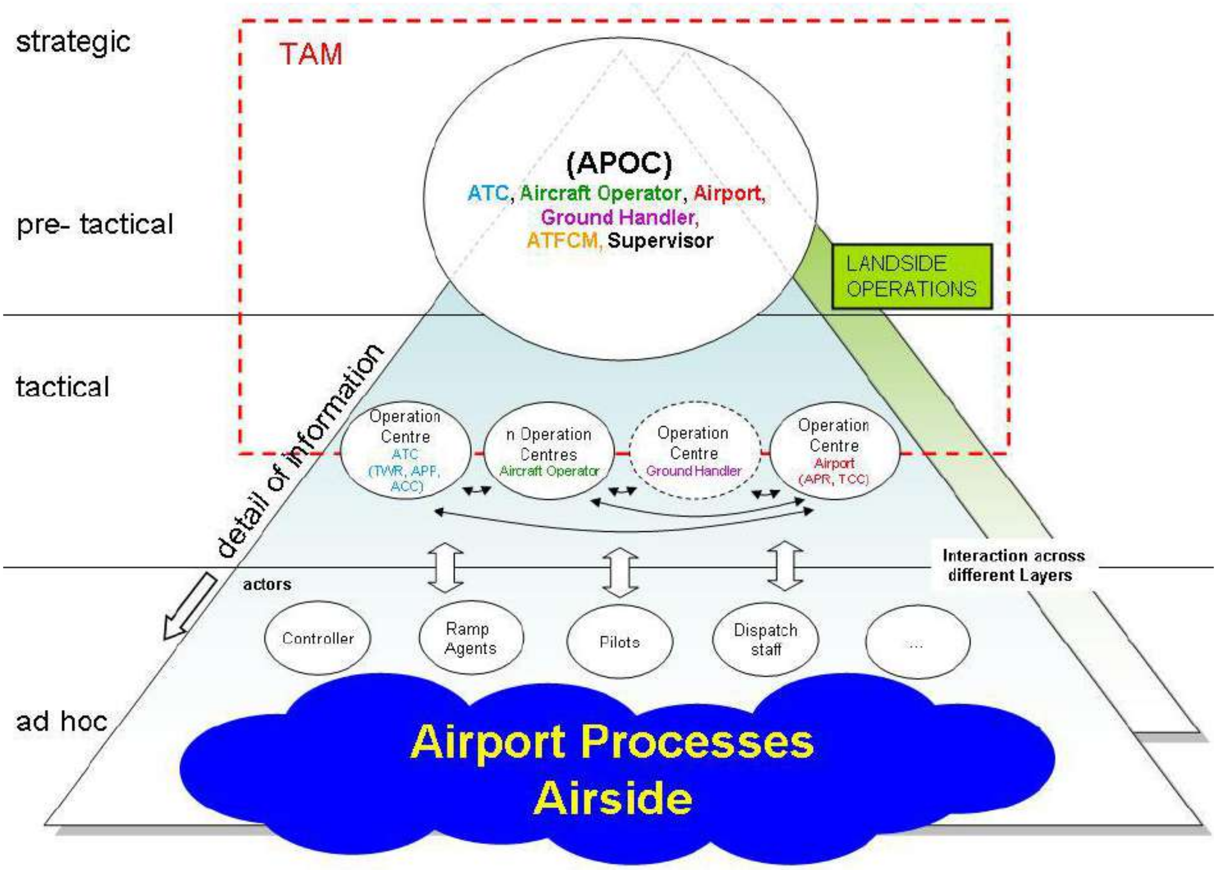

strategic
pre- tactical
tactical
ad hoc
TAM
(APOC)
ATC, Aircraft Operator, Airport,
Ground Handler,
ATFCM, Supervisor
LANDSIDE OPERATIONS
detail of information
Operation Centre ATC (TWR, APP, ACC)
n Operation Centres Aircraft Operator
Operation Centre Ground Handler
Operation Centre Airport (APR, TCC)
Interaction across different Layers
actors
Controller
Ramp Agents
Pilots
Dispatch staff
...
Airport Processes Airside

Figure 4.3: Hierarchical view of centres and actors within their appropriate time window (29)

5 Rules, policies, security and safety procedures in airports

Aviation safety and security is a combination of human and material resources to safeguard civil aviation against unlawful interference. According to ICAO's Annex 17, the relevant European and National Aviation Security legislation, relevant literature, the national security programs, and the input received from the consortium partners the most common aviation security and safety breaches and vulnerabilities include among others:

- Man-made (cyber & physical):
    - Physical access control breaches/administrative controls: It can refer to passengers, people other than passengers or vehicles gaining unauthorized access into an airport's-controlled area (security restricted areas and critical parts), perimeter event or breach, sterile area access event, etc. This breach refers to the failure in the processes of verification of identity or authorisation. Breaches in authentication include identity fraud, and breaches of physical access controls or administrative controls, include bypassing of an authentication check, thereby gaining access to a new attack surface.
    - Lack of appropriate level of physical security at facilities that house air traffic control systems and the management of security for operational computer systems.
    - Improper/no screening: It has been shown that airport checkpoint screeners might not adequately detect dangerous objects, and long-standing problems affecting screeners' performance remain, such as the rapid screener turnover and the insufficient screener training. In addition, as no screening takes place at landside areas the following incidents might occur:
        - Deadly/dangerous item, dangerous goods incident: It refers to conventional X-ray screening of checked baggage, which has performance limitations and offers limited protection against a moderately sophisticated explosive device.
        - Bombs, chemical/biological/radiological/nuclear (CBRN) threat or incidents.
    - Compromised employees/insiders: Especially in an airport environment, these pertain to individuals who exploit their knowledge or access to the airport, airline, or airport's assets, for unauthorised purposes. The insiders could be anyone, including an employee, contractor, consultant, or anyone else who has legitimate access to the airport's information or assets. This problem is long lasting and hard to manage by taking into consideration the interdependencies and the complex ecosystem of an airport.
    - Human errors: For example, administrative IT personnel or network administrators may make configuration errors that negatively impact operations or security. IT personnel can introduce errors into systems, by entering incorrect information or data. Lost hardware, such as laptops containing sensitive data or authentication details (passwords, or VPN certificates) can introduce vulnerability and lead to subsequent attacks.
    - Insufficient training: Security awareness training program on plans, policies and procedures should be designed to avoid inappropriate actions that increase risk and enhance detection. Response, recovery and mitigation actions; however, personnel may inadvertently not correctly follow these due to insufficient awareness, negligence, or other reasons.

    - Suspicious items (e.g. unattended baggage) either in non-controlled (landside) or controlled areas. Suspicious individual(s) who seem out of place. It may include impersonating pilots, airport line personnel, law enforcement, security, or employees of companies, including using fake badges or vehicle decals.
    - Malicious actions such as denial of service, exploitation of software vulnerabilities, misuse of authority, network interception attacks, social attacks, malicious software on IT assets, physical attacks on airport smart assets (such as theft of damage of airport IT infrastructure), etc.
    - Disruptive or unruly passenger who fail to respect the rules of conduct at an airport or on board an aircraft and may potentially jeopardize the safety of other passengers or the flight. Cases of disruptive behaviour on flights have risen sharply over the past few years, forcing national and international aviation to push for change. IATA and the International Civil Aviation Organisation (ICAO) published new legal guidance on how to manage unruly passengers on flights.
  - Technological/technical problems such as equipment failure or misuse, fabrication, mechanical, corrosion, design malfunction, etc.
  - Natural disasters, such as earthquakes, extreme weather (e.g. flood, heavy snow, fog, fire, hurricane etc.), and pandemics, can impact the systems supporting critical airport operations etc.
  - Political/Social disruptions (e.g. civil unrest, strikes, demonstrations, military actions, invasion, and political instability) can impact the systems supporting critical airport operations, etc.

Currently, regulation (EC) No 300/2008 of the European Parliament and of the Council establishes common rules in the European Union to protect civil aviation against acts of unlawful interference. Unlawful interference includes acts such as terrorism, bombing, sabotage to aircraft or airport facilities, hijacking, communication of false threat, which can cause chaos at the airport, and aircraft accidents etc. The regulation implements the EC regulation 1998/2015. The regulation's provisions apply to all airports, all operators that provide services at the airports, all entities located inside or outside airport premises providing services to airports. ICAO's annexes 9 to 11, 14 and 17-18, along with nation-specific and airport-specific regulations establish standards and recommended practices, concerning air navigation, flight inspection, prevention of unlawful interference, training, communication equipment, emergency planning, air accident investigation, etc. (see Table 5.3).

Provided the aforementioned institutional framework, airports implement several security measures and technology solutions to deter, detect and react to physical attacks (30) (31) (32) (33)**.** More specifically, access control should rely on a combination of physical elements (perimeter protection, physical barriers/bollards, guards, portals, security lighting, alarm systems, intrusion detection systems, audio and video surveillance systems, etc.) and policies (asset classification, identification, authentication, authorization, access groups, credentials and credentialing, entry control techniques, such as password, pin, biometric identifiers etc.) to properly operate. Each airport operator should clearly define the airport's boundaries to enable the appropriate security measures to be taken in each of those areas. To this end, boundaries are set between landside, airside, security restricted areas, critical parts, and demarcated areas. In most cases, physical barriers, clearly defined, separate the different areas. Physical barriers include any objects that prevent access into a restricted area or through an entry portal. There are two common categories of physical barriers: admission control and perimeter control:

- The admission control barriers are those used at entry points to selectively allow people to pass through. The most common admission control barriers are swing doors, turnstiles, etc. that might be operated mechanically or electronically in conjunction with electromagnetic door locks, keypads, or other entry-point screening mechanisms.

- Perimeter control barriers establish a secure physical boundary around an area, and limit access to and from that area to admission control points (e.g. fences, doors, gates, etc.). They can be constructed from a variety of material, while a common and effective type of physical barrier for perimeter control is chain-link fencing with barbed wire.

Consequently, the airport operators should ensure that the access to the different areas at airports is controlled to prevent unauthorized entry. The crossing of the barriers by persons or vehicles is established by the airport operator in collaboration with the relevant Civil Aviation Authority and the Airport's Security Department. Access control measures for controlling entry to the secured areas must ensure that: (a) only those individuals authorized to have unescorted access to the secured area are able to gain entry; (b) an individual is immediately denied entry to a secured area when that person's access authority to the area is withdrawn, and; (c) provide a means to differentiate between individuals authorized access to an entire secured area and individuals authorized access to only a particular portion of a secured area.

Measures for the screening of persons other than passengers and the examination of vehicles (vehicles entering critical parts or security restricted areas other than critical parts) should also be defined. Barriers that are not combined with intrusion detection equipment may be vulnerable to attack and unauthorized access if it is not under constant surveillance by security personnel. The surveillance, patrols, and other controls including technology using alarms and/or CCTV systems, lighting, sensors to detect climbers or cutting actions, and/or security force personnel such as staff dedicated to carry out surveillance activities are some indicative measures.

The aircraft security check is the responsibility of the owners or operators. Based on ICAO, each Contracting State shall ensure that aircraft security checks of originating aircraft engaged in commercial air transport movements are performed or an aircraft security search is carried out. A thorough inspection of the interior and exterior of the aircraft for the purpose of discovering suspicious objects, weapons, explosives or other dangerous devices, articles or substances is needed to be conducted.

Each airport operator should also ensure that the passengers and their cabin baggage are screened prior to boarding an aircraft departing from a security restricted area. Airport operators need to address the risk from weapons, explosives in liquid, aerosol or gel form, or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, from being introduced on board an aircraft engaged in civil aviation by implementing the restrictions and the associated measures recommended by ICAO. In addition to this, the commercial air transport operator is normally responsible for ensuring that only items of hold baggage which have been individually identified as accompanied or unaccompanied screened to the appropriate standard and accepted for carriage on that flight by the air carrier, are transported. This type of baggage should be recorded as meeting these criteria and authorized for carriage on the flight. Also, all cargo, mail, and other consumables and supplies must be physically screened before being loaded onto an aircraft. The means of screening include among others security scanners, shoe explosive detection, shoe metal detection, explosive trace detection equipment, x-ray equipment, hand-held metal detectors, walk-through metal detectors, physical searches, advanced cabin baggage x-ray, liquid explosive detection systems, remote explosive scent tracing and free running explosive detection dogs, cargo x-ray screening equipment, etc.

The security personnel provide all basic security services and their role is of paramount importance to maintain the best quality of security services. Their role includes among others the hold baggage screening, the security screening of all departing passengers and their baggage, the CCTV monitoring, the reporting of incidents, the patrolling of the different airport's areas (e.g. apron, aircraft parking areas, etc.), the control of access to areas at airports in order to prevent unauthorized entry, the response to alarms or unauthorized entry, the initiation of the communications with emergency response personnel in case that it is needed. To that end, their training should be continuous and motivational. A security awareness program shall be developed for security personnel and for airport employees. A hiring policy should be defined and as such background investigations shall be conducted for new hires and periodic updates for current employees should also be implemented (especially for those with access to secure areas). The security personnel and fast response teams shall have the right equipment at their disposal. For example, a real time communication system and emergency evacuation and protection systems shall be provided to security personnel to assist them to protect the passengers and employees.

The measures for handling special categories of passengers include among others the requests to allow armed personnel to travel, the measures and procedures to be taken in order to ensure safety on board when passengers subject of judicial or administrative proceedings are obliged to travel, the handling of disabled passengers and patients, etc.

In addition to the aforementioned, an airport as any other Critical Infrastructure must provide the required levels of physical security in order to protect people, data, equipment, systems, facilities and company assets in the case of any natural disaster, accidental event, explosion or sabotage. The methods must include among others, the appropriate site design and layout, analysis of environmental components, established physical security program, emergency response readiness, specialized and continuous training, power and fire protection systems, physical controls (e.g. perimeter security, motion detectors, etc.), technical controls (e.g. smart cards for access control, physical security intrusion detection systems, etc.), business continuity or disaster recovery plans to reduce business interruption, suppression systems in order to extinguish heat, oxygen, fuel, chemical reaction, etc. (34). The following Table 5.1summarises the most common measures discussed in the previous paragraphs.

Table 5.1: Most common physical security measures and technology solutions

Category	Measures/Actions
Physical (nontechnology) measures	Guards, port gates, fences, barriers, turnstiles, vehicle barriers doors and locks, speed bumps, roadway design, increased gate visibility/detection, perimeter reflectivity and signage, law enforcement or contract personnel continuously patrolling the airports' perimeters and areas, security buffer zones, clear zones for perimeter, inner/outer perimeter roads, name/nomenclature for areas of the perimeter, etc.
Physical (technology) measures	CCTV, video analytics, automated gate barriers, thermal imaging video, radar systems, light detection and ranging systems, passive infrared area sensors, physical and remote sensors, remote power/communications technology, alarms, perimeter intrusion detection systems, access control systems like the mantrap, biometric readers (fingerprint, iris scanners, etc.), fire detection systems/sensors, anti-piggybacking systems, mobile surveillance towers, lighting, badge readers, verification of authenticity by embedding specific technology to badges (guard against the use of fraudulent credentials), doors with access controls, etc.
Screening of passengers/employees, cabin baggage, hold baggage, cargo, in-flight catering, and supplies	Security scanners, shoe explosive detection, shoe metal detection, explosive trace detection equipment, x-ray equipment, hand-held metal detectors, walk-through metal detectors, physical searches, advanced cabin baggage x-ray, liquid explosive detection systems, remote explosive scent tracing and free running explosive detection dogs, cargo x-ray screening equipment, etc.
Operational efforts	Police presence (either stationed or patrols), K-9 teams, anti-terrorism teams (covert and overt elements), mobile explosives detection screening teams, visible intermodal prevention and response teams, security awareness (e.g., training, exercises), unpredictable police patrols, routine security inspections,

Category	Measures/Actions
	routine patrols (by the asset owner), monitor security cameras, security drills and exercises, etc.
	Aviation security staff and airport employees need to be carefully selected and properly trained and supervised to ensure that they are consistently able to carry out their duties in a highly proficient manner. Pre-employment background checks are needed, and specific security training of aviation security staff should be in place. Airport operators should develop, execute, and perform routine training and security awareness programs for their staff, including methods for the identification of suspicious persons, awareness of their responsibilities, the security procedures, and the relevant contacts. Reward programs for discovering breach suspects
	An airport security program (ASP) must, among other things, provide for the safety and security of persons and property on an aircraft against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary device onto an aircraft. Airports need to implement and maintain quality controls in their airport security programmes to determine compliance with and to validate the effectiveness of the programme.

As indicated in section 4.1, airports may endure a wide variety of malicious attacks of both physical and cyber nature. In this context, given the rapid evolution of and penetration of technological means into airports operation as a measure to cope with the ever increasing traffic and security needs, cyber-attacks are emerging, especially with the increasing use of Information Systems (IS).In this regards it should be taken into consideration that successful attacks on aviation/airport system(s) (through malicious exploitation of identified vulnerabilities) can disrupt air traffic and paralyse the airport operations with significant impacts on reputation and economy both on a local as well as national scale.

Looking at the detection of threats, solutions are available which are known as intrusion detection systems. These systems are attack warning systems that alert pilots, air traffic controllers and/or technical and administrative personnel at airports/air navigation service providers if anything has been hacked or is doing something it should not.

There are adjacent fields of crisis management where coordination during the response phase is investigated (35). Many crises involve interfacing diverse crisis management systems and solutions. Major crises can also frequently involve more than one country or region, which may have differing crisis management infrastructures and cultures. It is also highly likely that interfacing different systems and combining different solutions is necessary. Solutions used in crisis management must therefore be capable of meeting multifaceted challenges and delivering solutions that are modular, flexible, and adaptable.

The solutions must be tested and validated in realistic environments; they must be evaluated to assess their true benefits and for their overall suitability, before being adopted by end-users. Failure to meet these needs could result in less than perfect solutions being introduced or in the increased costs of crisis management capability development, due to the imperfect management of ever more complex crises. In the lack of yet existing and proven technologies to mitigate impacts of attacks, it is then important to utilise those measures which can prevent attacks from being successful:

- Build and promote security culture.
- Build increased security layers around the networks, which are more and more capable for interconnectivity with other systems and networks.

- Aviation industry must not forget the basics and cyber and physical security best practices.
- Strong identity and access management with privileged access security is a must to ensure only authenticated users have access to critical systems.
- Multifactor authentication must be enabled and used for all privileged access.
- Perform event analysis, recreate the attack scenario, and begin the remediation processes. Strengthening the ability to respond on technical and managerial levels.

Further improvements would be gained with a thorough risk assessment between participating entities, original equipment manufacturers, airlines and the aftermarket. This would include large scale exercises, tabletop exercises, penetration testing, or "red teaming," where attackers try to gain access to a system, as well as vulnerability testing, where they look for flaws in security. The overall approach includes steps such as: to look at planes, air-traffic control, airports and all the other elements of aviation infrastructure as an information system, to understand their strengths and weaknesses, then to inspect them frequently.

While many commercial businesses, such as the banking and healthcare industries, have beefed up cyber security measures, the aviation industry needs to keep pace. According to leading manufacturers in the field of aviation the aviation industry should implement a layered approach to cyber security, which use several defence mechanisms such as access restrictions, two-factor authentication, encryption, proactive threat hunting, insider threat monitoring, and managed detection and response (36). Other industry decided years ago that it was not sufficient to merely devise elaborate protections. "We must have some real-time capabilities to detect and respond" if an intrusion is under way (37).

The different assessments of the industry's vulnerabilities – and what leaders should do to combat future attacks – partly reflects the uncertain nature of threats. Industry officials agree there has not been a single verified instance of safety systems being breached on a large commercial jetliner. But at the same time, experts' warnings are getting louder about the dangers of attackers finding vulnerabilities in aviation protections. In any case, for combating the possibility of vulnerabilities being exploited, airports have standardised their mitigating stance though the formulation of strategies for achieving high levels of security both in the cyber and physical domains. These strategies aim through accurate mapping of the underlying systems and stakeholders to identify any weaknesses in the relevant daily operations.

As reported in (38) the ICAO (with ICAO/A39) calls on states and industry stakeholders to encourage coordination with regard to aviation cyber and physical security strategies, policies and sharing of information to identify critical vulnerabilities that need to be addressed, by developing systematic information sharing on cyber and physical threats, incidents and mitigation efforts (39). (38) summarises that existing vulnerabilities in airport ICS have been evaluated by US Airport Cooperative Research Program and a Guidebook on Best Practices for Airport Cyber security has been published in 2015, to mitigate inherent risks of cyber-attacks on technology-based systems (40).

In 2016, ENISA also published security guidance for smart airports (21), presenting key stakeholders, asset groups, threats and risk analysis, best practices and security recommendations for physical and cyber security controls addressed to airport decision makers, policy-makers and industry stakeholders. Afify et al. then focus on analysing Denial of Service (DoS) attacks that occur in airports and especially in their automation systems by describing how attacks are launched along with effective countermeasures (41). Finally, SESAR research addressed cyber security issues in Airport Operation Centres including a comprehensive maturity model to approach cyber-security within European ATM and to develop a comprehensive response to cyber-threats (42). In addition, Airports Council International (ACI) has launched a new guidance handbook on business continuity management to help airport operators to develop appropriate plans that take account of a wide range of possible events, to enable them prepare and cope with a disruption, and to return to normal operations as soon as possible (43).

Although threats to smart airport’s apply to broad categories of assets (such as communication networks, servers and control systems, internal/sensitive information, authentication and access control systems), the majority of researchers focus on one or two scenarios of attack, while addressing security issues in airports. (38) conclude, that no one has presented a complete scenario analysis of malicious attacks that may happen in smart airports, concerning IoT technologies and smart applications, including mitigation actions, resilience measures and impact effects on the information security triad (Confidentiality-Integrity-Availability: CIA), while in their survey they included an analysis of seven different combined attacks, the affected assets, the following cascading effects, the possible mitigation actions and the needed resilience measures has been conducted. Although significant research has been presented regarding ATM risks, there is a lack of research about threats and vulnerabilities for ground handling IT systems and airport services, especially when equipped with smart applications.

In this context, SATIE encompasses distinct scenarios combining cyber-physical threats against broad categories of systems (i.e. access control, Flight Information Display System (FIDS), Public Announcement system (PA), Automated Border Control systems (ABC), Airport Operation Control system, Resource Management System (RMS), Baggage Handling System (BHS), passenger transportation system, and structural elements) as described in detail in deliverable D2.1. The aim is to investigate an as wide range as possible of operational situations and circumstances that could be met during the onset of a malicious activity against critical airport infrastructure.

In this chapter, the rules and policies (section 5.1), as well as the resilience and maintenance procedures (section 5.2) are presented.

5.1 Rules and policies

The following tables (Table 5.2, Table 5.3) present the cyber and physical rules and policies, selected for addressing the security and safety needs of SATIE. This is not an exhaustive list of all available rules and policies but a refined selection of those considered to best suit the needs of the projects’ activities and systems of interest. The presentation of the information is organised around the three main Operational Phases (OP): before the crisis, during the crisis and post crisis.

Table 5.2: Cyber rules and policies

Article/Regulation	OP1 - Before the crisis	OP2 – During the Crisis	OP3 – Post crisis	Critical Systems - Assets
NIST Framework for Improving Critical Infrastructure Cybersecurity	**Identify** Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management **Protect** Identity Management and Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology	**Detect** Anomalies and Events Security Continuous Monitoring Detection Processes	**Respond** Response Planning Communications Analysis Mitigation Improvements **Recover** Recovery Planning Improvements Communications	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft
ISO 27001:2013 (44) Information technology	4.2 Establishing and Managing the ISMS. 5.2 Resource Management Controls Objective: A5 Security Policy A10.4 Protection against malicious and mobile code A10.5 Backup/Restore A10.6 Network Security Mgt. A10.7 Media Handling A10.10 Monitoring A11.5 Operating System Access Control A13 Information Security Incident Mgt. A14 Business Continuity Mgt.	A6.2 External Parties A9 Physical & environmental Security A9.2 Equipment Security A10 Communications & Operations Mgt. A10.2 Third Party Service Delivery Mgt. A10.4 Protection against malicious and mobile code A10.10 Monitoring	A10 Communications & Operations Mgt. A10.2 Third Party Service Delivery Mgt. A10.5 Backup/Restore A10.6 Network Security Mgt. A10.10 Monitoring A11.5 Operating System Access Control A7 Asset Management A7.2 Classification. A13 Information Security Incident Mgt. A14 Business Continuity Mgt.	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft
ISO 31000:2018 (45) Risk management - Guidelines	Asset Identification Risk Identification Risk Analysis Risk Evaluation Risk Treatment	Communication and Consultation	Monitoring and review	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft

Article/Regulation	OP1 - Before the crisis	OP2 – During the Crisis	OP3 – Post crisis	Critical Systems - Assets
ISO 27005:2018 (46) Information technology -Security techniques - Information security risk management	8 InfoSec risk Assessment 9 InfoSec risk Treatment 12 Infosec Risk Monitoring & Review	-	-	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft
ISO/IEC 27033:2015 (47)- IT network security standard.	The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections.			FIDS, ABC, PA, AOC, BHS, ATC, aircraft, passengers, employees.
ISO 22301:2019 – Societal Security (48)	It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, and prepare for disruptive incidents when they arise.	It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to respond to disruptive incidents when they arise.	It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to recover from disruptive incidents when they arise.	FIDS, ABC, PA, AOC, BHS, ATC, aircraft, passengers, employees.
ISO/IEC 27002:2013 (49) Information technology – Security techniques — Code of practice for information security controls	Establishing Information Security Implementation of Information Security Policies Access Control Cryptography Physical and environmental security Supplier relationships - Information security in supplier relationships and Supplier service delivery management	Information security incident management - Management of information security incidents and improvements Information security aspects of business continuity management - Information security continuity and Redundancies	Operation Security- procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination Communication security - Network security management and Information transfer	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft
EU NIS directive (50)	Implementation of Information Security Policies	-	-	FIDS, ABC, PA, AOC, BHS, ATC, passengers, employees, aircraft
EUROCAE ED-201 – 204 Aeronautical Information Security	Aeronautical Information System Security Framework. Airworthiness Security Process. Airworthiness Security Methods			AOC, ATC, passengers, employees, aircraft

Article/Regulation	OP1 - Before the crisis	OP2 – During the Crisis	OP3 – Post crisis	Critical Systems - Assets
System (AISS) (51)	and Considerations. Instruction for Continued Airworthiness			
ARINC (51)	ARINC 664. Specification for a deterministic aircraft data network bus for aeronautical, railway and military systems. Based on standard IEEE 802.3 extended by adding Quality of Service (QoS) and deterministic behaviour with a guaranteed dedicated bandwidth. AFDX network.			AOC, ATC, passengers, employees, aircraft

Table 5.3: Physical rules and policies

Article/Regulation	OP1 - Peacetime and preparedness (before the crisis)	OP2 - Early threat detection (during the crisis)	OP3 - Incident response and decision making (post-crisis)	Critical Assets
ICAO's Annex 17 Security - Safeguarding International Civil Aviation Against Acts of Unlawful Interference	Article 2.3: International Cooperation Article 2.4: Equipment, Research and Development Article 3.1: National Organization and Training Article 3.2.1: Airport Security Program Article 3.2.3: Airport Security Committee Article 3.2.4: Contingency Planning and Exercises Article 3.2.6: Architectural and Infrastructure Requirements Articles 4.3 -4.7: Implementation of Aviation Security Measures	Article 5.2: Response to an act of unlawful interference	Article 5.3: Exchange of Information and Reporting	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
ICAO Aviation Security Manual – Document 8973 (Restricted Access)	This manual assists member states on implementing Annex 17 of the Chicago Convention. It is regularly reviewed and amended as new threats and technological developments are identified and it provides guidance on how to apply its Standards and Recommended Practices.	This manual assists member states on implementing Annex 17 of the Chicago Convention.	This manual assists member states on implementing Annex 17 of the Chicago Convention.	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft

Article/Regulation	OP1 - Peacetime and preparedness (before the crisis)	OP2 - Early threat detection (during the crisis)	OP3 - Incident response and decision making (post-crisis)	Critical Assets
Attachment to Annex 17 from ICAO's Annex 2 "Rules of the Air"	-	Article 3.7: Notification to Air Traffic System (ATS) Article 2.2: Broadcast warnings on the VHF emergency frequency	-	
Attachment to Annex 17 from ICAO's Annex 6 "Operation of Aircraft"	Article 13.1: Security of the flight crew compartment Article 13.2: Aeroplane Search Procedure Checklist Article 13.3: Training Programs	-	Article 13.4: Reporting acts of unlawful interference	Aircraft, employees, passengers
Attachment from ICAO's Annex 9 "Facilitation"	Article 3.33: Valid passports or other acceptable from of identify Article 4.17: Approved Custom offices Article 4.48: Imported Security Equipment - ground equipment Article 6.1: Satisfactory Facilities and Services Article 6.2.2: Specialized communication equipment	-	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
Attachment from ICAO's Annex 10 "Aeronautical Telecommunications"	-	Article 2.1.4: Mode A reply codes (information pulses)	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
Attachment from ICAO's Annex 11 "Air Traffic Services"	-	Article 2.22: Service to aircraft in the event of an emergency Article 5.1: Alerting Service Article 5.2: Notification of Rescue Coordination Centres Article 5.5: Information to the Operator Article 5.6: Information to aircraft operating in the vicinity of an aircraft in a state of emergency	Article 5.11: Investigation - Informing Aviation Security Authorities	Aircraft, employees, passengers

Article/Regulation	OP1 - Peacetime and preparedness (before the crisis)	OP2 - Early threat detection (during the crisis)	OP3 - Incident response and decision making (post-crisis)	Critical Assets
Attachment from ICAO's Annex 14 "AERODROMES"	Article 3.13: Isolated aircraft parking position Article 5.3: Lights / Security Lighting Article 8.1: Secondary power supply Article 8.4: Fencing / Patrolling Article 9.1: Aerodrome Emergency Planning Article 9.1.12: Aerodrome Emergency Exercise	Article 9.1.7-9.1.10: Emergency Operations Centre and Command Post Article 9.1.11: Communication System	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
Attachment from ICAO's Annex 18 "The Safe Transport of Dangerous goods by Air"	Article 2.2: Dangerous Goods Technical Instructions Article 10: Establishment of Training Programs	-	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
EU Regulation 300/2008 Most Recent Version Implementing Regulation 1998/2015	Article 1.1: Airport Planning Requirements Article 1.2: Access Control Article 1.3: Screening of Persons other than Passengers Article 1.4: Examination of Vehicles Article 1.5: Surveillance, Patrols and other physical controls Article 1.6: Prohibited Articles Article 3: Aircraft Security Article 4: Passenger and Cabin Baggage Screening Article 5: Screening of Hold Baggage Article 6: Cargo Security Article 7: Air-Mail Security Article 8: In-Flight Supplies Article 9: Airport Supplies Article 10: Security During Flight Article 11: Staff Recruitment and Training Article 12: Security Equipment	-	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
National Civil Aviation Security Regulation AND Security Technical Directives (Technical Directive No. 1, Technical	PART B Article 1. Airport Security Measures Article 2: Demarcated Airport Areas Article 3: Aircraft Security Article 4: Passenger and Cabin Baggage Screening	PART C Article 1. Handling of Security Threats and Incidents Article 2. Additional	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft

Article/Regulation	OP1 - Peacetime and preparedness (before the crisis)	OP2 - Early threat detection (during the crisis)	OP3 - Incident response and decision making (post-crisis)	Critical Assets
Directive No. 2)	Article 5: Screening of Hold Baggage Article 6: Cargo Security - Air-Mail Security Article 7: CoMat/CoMail (Company Materials/Mail) Article 8: In-Flight Supplies Article 9: Airport Supplies Article 10: Security During Flight Article 11: Staff Recruitment and Training Article 12: Security Equipment Article 13: General Aviation	Security Measures		
National Civil Aviation Training Program	Describes the National Policy on the Basic, Advanced and Expertee Aviation Security Training Courses Implemented by the Hellenic Civil Aviation Authority	-	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft
National Civil Aviation Security Audits and Inspections	Describes the methodology and the protocols for auditing / inspecting / testing the Airport Security System	-	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft

Article/Regulation	OP1 - Peacetime and preparedness (before the crisis)	OP2 - Early threat detection (during the crisis)	OP3 - Incident response and decision making (post-crisis)	Critical Assets
Airport Security Program	PART B Article 1. Airport Security Measures Article 2: Demarcated Airport Areas Article 3: Aircraft Security Article 4: Passenger and Cabin Baggage Screening Article 5: Screening of Hold Baggage Article 6: Cargo Security - Air -Mail Security Article 7: CoMat/CoMail (Company Materials/Mail) Article 8: In-Flight Supplies Article 9: Airport Supplies Article 10: Security During Flight Article 11: Staff Recruitment and Training Article 12: Security Equipment Article 13: General Aviation Article 14: Special Categories of Passengers Article 15: Weapons and Ammunitions	PART C Article 1. Handling of Security Threats and Incidents Article 2. Additional Security Measures	-	FIDS, ABC, Access Control, passengers, employees, facilities, infrastructure, equipment, aircraft

5.2 Maintenance procedures, including systems’ risk and resilience management and deprecation

Maintenance procedures, being a cornerstone towards reaching a high security level from both the cyber and physical points of view, should better consider infrastructure ageing including: systems’ risk and resilience management, deprecation over the time and their vulnerabilities, single nodes failure, resilience, and Mean Time Between Failures (MTBF) at system and system-of-systems level. The following sections analyse these aspects in the context of SATIE.

5.2.1 Risk and resilience management

Risk and resilience management plays a fundamental role in the project SATIE. The SATIE toolkit contains among others i) the risk assessment platform and ii) the simulation of impact propagation which both have an important role for risk and resilience management (see chapter 6).

Resilience in general has a broad variety of definitions. For example, the United Nations Office for Disaster Risk Reduction (52) defines resilience in the following way: “The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management.” Resilience is a time-dependent process and therefore a so-called resilience cycle can be introduced to characterize the different phases, e.g. (53). The resilience cycle contains, dependent on the definition, elements like ‘prevent’, ‘protect’, ‘respond’, ‘recover’ and ‘prepare’. The latter definition is closely linked to the crisis management cycle (see chapter 4) where it is distinguished into four phases, namely prepare, respond, recover and mitigate.

In this context, to prevent means to avert a danger; which requires well-modelled and known disturbances to design a robust system (54). If the impact of a threat on a system cannot be prevented, the damage should be minimized by protecting the system. The system responds to a threat and with the help of effective measures the degradation of performance is minimized. It should be noted though that the response depends on system properties that are in place before a surprising event happens (54). Recovery of the system means returning to normal operation, adapting and adjusting to the new situation after the disturbance and learning from the event. Lessons learned from any previous event should be considered in order to better understand and protect the system.

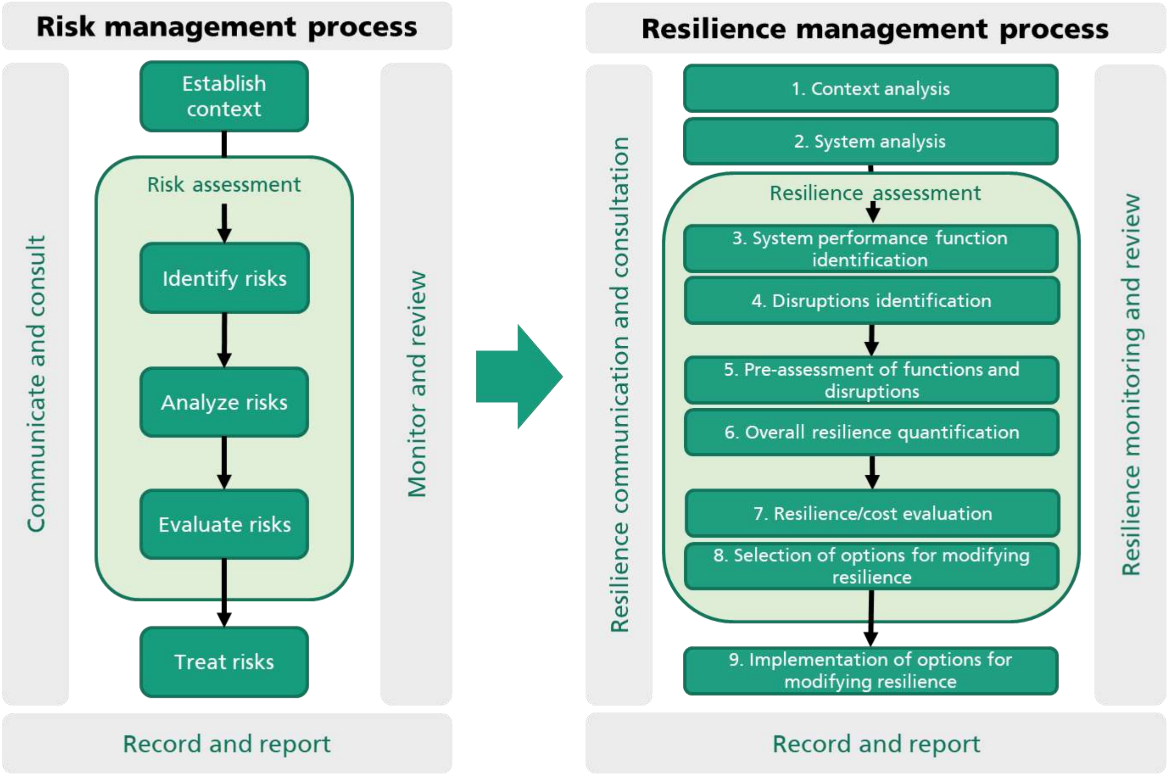

Risk management process
Establish context
Risk assessment
Identify risks
Analyze risks
Evaluate risks
Treat risks
Communicate and consult
Monitor and review
Record and report
Resilience management process
1. Context analysis
2. System analysis
Resilience assessment
3. System performance function identification
4. Disruptions identification
5. Pre-assessment of functions and disruptions
6. Overall resilience quantification
7. Resilience/cost evaluation
8. Selection of options for modifying resilience
9. Implementation of options for modifying resilience
Resilience communication and consultation
Resilience monitoring and review
Record and report

Figure 5.1: Risk and resilience management process. Left: Risk management process following ISO 3100. Right: Resilience management process that extends the risk management process and involves resilience specific steps. Reaching the last step of both processes which means changing the system, implies that the processes start again from the beginning (55).

However, resilience management can be derived from the risk assessment process which is based on ISO 31000 (2018) (56) and is shown in Figure 5.1 (left). It consists of 5 main steps, i.e. (1) context analysis, (2) risk identification, (3) risk analysis, (4) risk evaluation and (5) risk treatment. The resilience management process extends these five steps as is shown in Figure 5.1 right:

1. Context analysis: general description of the system and identification of stakeholders.
2. System analysis: analysis of system components, functions and interfaces for modelling.
3. Identification of system performance functions: definition of performance measures like e.g. combined performance indicators, so-called key performance indicators that represent the functionality of the system.
4. Identification of disruptions: analysis of threats, hazards and disruptions.
5. Pre-assessment of critical combinations: analysis of the combination of performance functions (step 3) with disruptions (step 4) to identify critical combinations.
6. Resilience analysis: system modelling and simulation of crisis events to determine resilience.
7. Resilience evaluation: comparison of resilience performance (evaluation of step 5 and 6).
8. Selection of mitigation options: comparison of different mitigation and improvement measures. This could be e.g. redundancies for system critical components, security and maintenance procedures, detection of threats and corresponding early warning.
9. Implementation and monitoring of mitigation options: choice of measures for implementation.

Specifically, the general outcome of step 6 is the quantification of the performance loss due to a potential crisis event, as illustrated in Figure 5.2. Thereby, the “resilience curve” covers all the resilience cycle phases (prevent, protect, respond, recover and prepare) as mentioned above. The simulation of resilience curves requires dedicated input, collected in the previous steps of the management process, such as system specifications (nodes and connections), the type of crisis events that need to be considered and the performance measures that should be used for the quantification (i.e. the y-axis of the "resilience curve"). Importantly, step 8 is strongly related to the impact propagation tool of SATIE, where potential improvement measures for the identified crisis event are tested and compared. The goal of the latter step is to minimize the area above the curve which is presented in light green in Figure 5.2. This means the amplitude and the duration of the impact should be as small as possible. Note that an impact on the performance may be delayed with respect to the crisis event and the recovery action due to the system's complexity leading to effects like inertia.

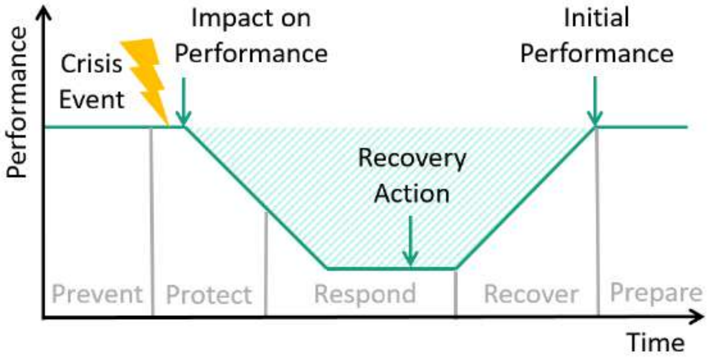


Figure 5.2: The green curve represents the system's performance as a function of time in the case of a crisis event. This resilience quantification corresponds to point 6 in the resilience management process of Figure 5.1.

Another important challenge when identifying measures and procedures to achieve resilience is the trade-off between objectives. A system could be very resilient but would be e.g. located in a very remote area that is not economical. This means that not every measure that keeps the system secure is useful and this must be reflected in the performance indicators. Assuming the performance is quantified appropriately considering the latter constraints, e.g. Monte-Carlo simulations could be employed to identify the best strategy available to maintain the system's resilience.

The nine steps of the resilience management process will be further adapted to fit the scope of the project SATIE and to support the simulation of impact propagation. This will be further discussed in the deliverable D2.5.

5.2.2 Systems' deprecation

The following sections will detail facets of systems' deprecation.

5.2.2.1 Hardware assets ageing

The hardware components of an information system have a limited lifetime and the ageing of these components leads necessarily to failure after a duration that is unknown in advance. The failure of a hardware component has in general a high impact, mitigated by the role of the component: failure of a keyboard does not have the same impact as the failure of a hard disk storing the AODB. Estimating the time at which a hardware component will fail is therefore of primary importance in predictive maintenance. This time being of course impossible to know precisely, only estimation based on statistics and probability can be obtained. Two statistical data, used in reliability engineering, capture this estimation:

- **Mean Time Between Failure (MTBF)** for repairable systems or **Mean Time to Failure (MTTF)** for non-repairable systems: average mean time between failures (for repairable systems) or average time up to failure.
- **Failure rate (usually denoted λ)**: frequency, in failures per unit of time, at which a system fails.

However, failure rate (and hence MTBF) is not constant over time and most of the time it follows a curve as presented in Figure 5.3, known as the "bathtub curve", which comprises a first decreasing failure rate (*early*), a second constant failure rate (*random*) and a third increasing failure rate (*wear-out*).

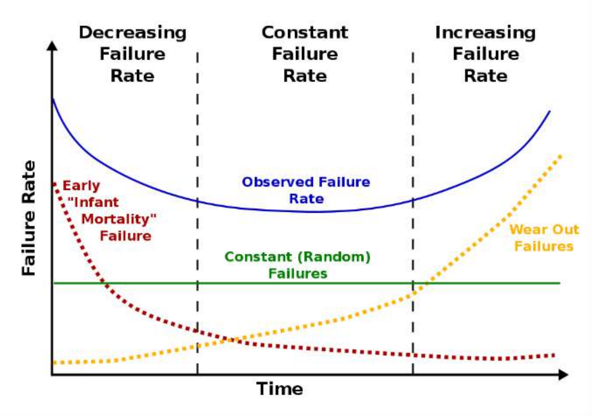


Figure 5.3: The bathtub curve of failure rate

5.2.2.2 Use of inventory for hardware assets lifecycle management

In order to setup a preventive maintenance policy against assets ageing and induced failures, establishing an inventory of hardware assets is mandatory. Several solutions for IT Service Management (ITSM) allow tracking of the life cycle of hardware components of the information system in a precise way, including build time, constructor's data, dates and reasons of failures. For instance, Teclib's GLPI solution for ITSM adopts for hardware assets a predefined lifecycle workflow as presented in Figure 5.4.

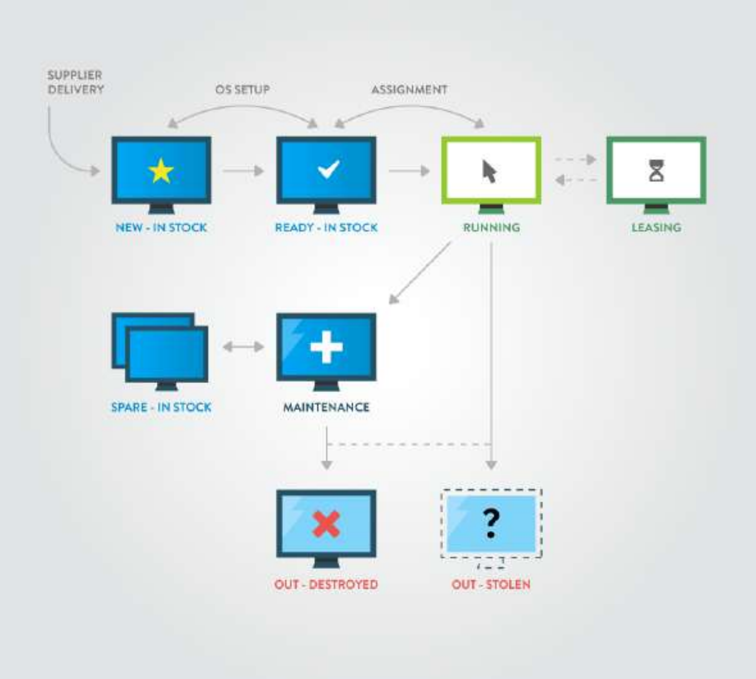


Figure 5.4: Hardware asset lifecycle in GLPI

5.2.2.3 Software assets deprecation over time

Although software assets do not follow the same ageing related hazards, predictive maintenance must consider the fact that software is supported by its editor for a limited amount of time, the main impact being the end of *security updates*.

An edifying illustration on the impact of the end of security updates is the WannaCry[1] attack: WannaCry ransomware targeted Windows system via the EternalBlue[2] exploit. A security bulletin and associated patches was issued by Microsoft on March 14, 2017. However, this patch was only for supported versions of Windows at that time, which excluded Windows XP and Windows Server 2003. Software editors follow their own lifecycle, for instance two major operating systems providers:

- Microsoft Windows 10 Enterprise is serviced for 18 months or 30 months, depending on semi-annual channel[3].
- Ubuntu Linux Long Term Support releases receive maintenance updates for 5 years[4].

Enabling predictive maintenance for software must therefore take into account these data; however, upgrading an operating system is often a complicated task because of legacy applications, i.e. applications for which editors do no longer supply new releases and that are dependent either on an deprecated operating system or on a specific hardware that is not supported by the operating system vendor.

[1] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[2] https://en.wikipedia.org/wiki/EternalBlue

[3] https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

[4] https://ubuntu.com/about/release-cycle

5.3 Airports’ Operations Centres

Current developments in SESAR foster the implementation of an airport operation centre at any airport. As already suggested by the name, the centre focuses on enhancing airport operations by coordinating different airport stakeholders. So consequently, these stakeholders are primarily involved in the regular operations to process scheduled flights on time. That said representatives of major airlines, ground handlers, the airport authority and the air navigation service provider are forming the core team of the AOC whose theoretical background is thoroughly presented in section 4.3. In case of a security incident, additional stakeholders must be involved in the coordination process. Depending on the nature of the incident, different stakeholders (police, Rescue Fire Fighting Services (RFFS), rescue teams, IT experts, military, governmental representatives, engineers, etc.) might be activated. Whether they join the team in a physical environment like an ops room or if they join in via a virtual centre is a question of implementation. The first case fosters the direct contact while the latter case is faster, because some of the stakeholders might not be located in the vicinity of the airport.

In case of a security incident the following agenda is proposed to optimize reaction efficiency and reaction speed:

- Security incident detection.
- Depending on the nature of the attack, the required stakeholders are determined.
- Immediate meeting of these stakeholders in an AOC (either face to face or virtual).
- Common decision about response and recovery measures.
- Execution of the response and recovery measures by each partner.
- Common monitoring of effectiveness in the AOC.
- If necessary, adaption of response and recovery measures.

The main operations executed by the AOC at the participating airports, the various activities coordinated by the AOC, the safety and security procedures, and its role in case of an emergency, are considered confidential information and as such are not intentionally included in this report.

6 Common and holistic security and safety agenda

As already outlined in the previous sections, there are many current standards and several different guidelines for crisis management. A plethora of security measures are adopted in airport infrastructure to maintain the physical and cyber security of the passengers. However, there are still some gaps, and these are very representative of today's challenges in cyber and physical security of the airports.

From the analysis conducted in the previous sections, it appeared that it is crucial for airports to have a holistic physical and cyber crisis management process that explains how internal and external stakeholders cooperate and exchange information in a unified manner. In addressing this need, in the following paragraphs, a holistic physical and cyber crisis management process is presented. The stakeholders involved are identified and analysed in section 6.1, based on those described in section 4 and further updated by SATIE operators/end-users. The interactions of the stakeholders in the four concurrent and continuous crisis management phases (preparedness, response, recovery and mitigation) are presented in section 6.2.

Finally, SATIE proposes a holistic approach by developing an interoperable toolkit which also improves situational awareness at airports and cooperation among different stakeholders. Having a shared situational awareness, security practitioners and airport managers collaborate more efficiently to the crisis resolution. Emergency procedures can be triggered simultaneously through an alerting system in order to reschedule airside/landside operations, notify first responders, cyber/physical security and maintenance teams towards a fast recovery. In the context of SATIE, the Crisis Alerting System will enhance the airport operations by coordinating different airport stakeholders.

6.1 Airports' crisis management stakeholders

During the crisis management, several stakeholders that have different needs and requirements, get involved in the process, trying to cooperate, respond and support recovery and impact mitigation. Security stakeholders can be categorized according to their involvement and perceived proximity to the organization into internal and external, as further analysed below.

Internal stakeholders are these entities designated with duties and responsibilities within the organization's environment, play a role to its performance and can affect or can be affected by decisions made. Based on relevant literature review and information collected from the participating airports, the following list (Table 6.1) summarises the internal stakeholders in the context of SATIE.

Table 6.1: Airports' crisis management internal stakeholders

No	Stakeholder	Short Description
1	**Airport's Board of Directors (ABoD)**	The Airport company representatives.
2	**Data Protection Officer (DPO)**	The primary role of the Data Protection Officer is to ensure that organisational processes and the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) follow the applicable data protection rules. In the EU institutions and bodies, the applicable Data

No	Stakeholder	Short Description
		Protection Regulation (Regulation (EU) 2018/1725) obliges them to appoint a DPO.
3	**Airport Duty Officer (ADO)**	The ADO is responsible for managing daily operations, entitled by the airport operator in order to assure that the airport is operated in accordance with its national licensing conditions and international regulations. In case of emergency, ADO's responsibilities include among others: • Assessment of the incident's criticality. • Activation and coordination of the Crisis Management Centre (CMC)/Crisis Management Team (CMT) or Emergency Operations Centre (EOC)/Emergency Operations Team (EOT). • Ensuring the best interest of passengers and airlines are met Take appropriate decisions to remove any alert/warning under their sole area of responsibility.
4	**Physical security manager/ personnel**	The main role of the physical security manager/security personnel is to develop and implement security policies, protocols and procedures, manage training of security officers and guards (internal and external), plan and coordinate security operations and staff when responding to alarms and emergencies, all related to the physical part of security. During a crisis, the physical security manager handles the aspects of the incident that are linked to the physical access to the premises and the physical protection of the infrastructure.
5	**IT Security manager/ personnel**	The IT security manager/security personnel are responsible for leading and managing all relevant activities of the information security risk assessment and security operations team (implementation, installation, monitoring and service/support of airport's IT infrastructure such as networks, platforms, applications, devices etc.); develop, assess, update and enforce security plans and policies in accordance with IT policies, standards, and compliance requirements; respond to cyberattacks; mitigate cyber risks; provide reports on security issues/threats; and train IT and other personnel. This person will manage the incident as soon as it is brought to their attention until it has been contained and remediated. They will liaise with airport's management, and possibly with other internal and external staff to handle the incident. This person has to have knowledge about the organisation's business activities because they will be the first one to make business decisions during a cyber-crisis.
6	**Technical manager/ Technical staff**	The technical manager/staff is responsible for identifying, managing and maintaining the technical components of the organization, such as energy, elevators, technical gas/fluid, temperature, air control systems or building management; manage physical access rights, SCADA systems, natural hazards and safety events to the organizations infrastructures and processes. They should have good knowledge of the ICT infrastructure as they will be responsible for the investigation and confirmation of the incident and development of technical solutions to manage the incident.

No	Stakeholder	Short Description
7	**Crisis Management Centre (CMC) / Crisis Management Team (CMT)**	The Crisis Management Centre/Crisis Management Team is activated and coordinated by the ADO. Their main responsibilities include the following among others: • Provide support to the ADO during crisis management. • Assess incident's criticality. • Activate internal/external stakeholders in order to respond to the crisis. • Assure appropriate communication and coordination with relevant stakeholders. • Apply relevant procedures and plans in order to respond to the crisis, • Prepare crisis log files. • Evaluate the effectiveness of the response actions. • Provide information to the media.
8	**Airport Operations Centre (AOC)**	Supervision and management of all airport operations in order to assure the airport's seamless and safe operation. An operational management structure that permits relevant airport stakeholders to have a common operational overview and to communicate, coordinate and collaboratively decide on the progress of present and near-term airport operations. During a crisis the Centre has the following responsibilities: • Take appropriate actions to manage any situation that might lead to a crisis under their sole area of responsibility. • Notification of the ADO. • Notification of involved parties. • Coordination and supervision of involved stakeholders. • Take the appropriate actions in order to assure the airport's operation during crisis (if possible).
9	**Emergency Operations Centre (EOC)/ Emergency Operations Team (EOT)**	In the case of a major crisis situation, EOC/EOT will be activated by the ADO.
10	**Security Operations Centre (SOC)/ Security Services Department**	SOC is a dedicated site where enterprise Information Systems (applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended (24x7x365). As soon as soon as an incident is detected, they liaise with relevant internal stakeholders.
11	**IT department**	Members of the IT department are always present in the CMC during a crisis. These experts provide the proper function of all communication systems and information channels, thus avoiding any delayed or inappropriate flow of the information. They have technical knowledge about the organisation’s network (firewall, proxies, IPS, routers, switches etc.); as well as on the analysis/restriction of data flow in and out of the airport’s network.
12	**Media centre**	This is the centre where centralized information is released about the crisis. As the facility is fully equipped and suitable for briefings, they are also provided with regular updates on the situation, either by oral briefings, prepared handouts or status boards.

No	Stakeholder	Short Description
13	**Friends and relatives assistance centre**	During a crisis there is the likelihood that families, friends and relatives of crisis victims and participants may call, visit and/or remain at the airport until the situation is resolved. It is a specific area designated as the waiting area for friends/family members. These people are to be provided with at least the same information as the media, but preferably more (if possible).

Before, during and after a crisis and in order to more efficiently and effectively handle incidents, internal stakeholders should cooperate and exchange information with external ones. This category includes individuals or groups outside the organization that can affect or can be affected by a crisis, as they are conjoint into an interdependent relationship. The following Table 6.2 summarizes the external stakeholders to be considered in the context of SATIE (non-exhaustive list).

Table 6.2: Airports' crisis management external stakeholders

No	Stakeholder	Role
14	**International and EU Organisations (e.g. ICAO, EASA, EUROCONTROL)**	They provide international standards, regulations, standardisations and best practices for effective and efficient airport operations and crisis management. They also perform investigation and monitoring.
15	**Air Accident Investigation and Aviation Safety Board (AAIASB)**	The purpose of the National AAIASB is to reach and maintain the highest possible flight safety level in each country through aircraft accident investigation. The investigations that AAIASB conducts comply with ICAO Annex 13 and the E.U. Regulation 996/2010. Their mission is to find the factors that contributed to an accident or a serious incident and to issue the safety recommendations which after their implementation will prevent similar accidents from happening in the future.
16	**National Civil Aviation Authority (CAA) / Aviation Authority**	This is the national authority responsible for the development and implementation of the national security program.
17	**General Secretariat for Civil Protection (GSCP)**	GSCP is a national authority and its mission is to design, plan, organize and coordinate actions regarding risk assessment, prevention, preparedness, information and response to natural, technological or other disasters or emergencies; coordinate rehabilitation operation; monitor the above actions; and inform the public on these issues.
18	**National Authorities**	Ministry of Interior, Ministry of Transport, Ministry of Defence, Ministry of Foreign Affairs.
19	**National Intelligence Agency**	This is the national authority that is responsible for a range of domestic and foreign matters, ranging from criminal activities and civil rights violations, to terrorism and espionage.
20	**National Data Protection Authority**	Data protection law grants the data subjects (e.g. individuals), certain rights and imposes certain responsibilities on data controllers (e.g. anyone who keeps personal data in a file and processes it).
21	**Law Enforcement Agencies (LEAs) (e.g. Police)**	They activate operation plans and act accordingly. They are continuously trained and participate in tabletop and field exercises and simulations with passengers, staff, volunteers etc.
22	**Rescue Fire Fighting Services (RFFS)**	They activate their operational plans and act accordingly; they are equipped with the necessary equipment in accordance with ICAO

No	Stakeholder	Role
		requirements. They are continuously trained and participate in tabletop and field exercises and simulations with passengers, staff, LEAs, volunteers etc.
23	**Emergency medical services (ambulance) / First aid services**	Emergency (injured and casualties) transports to the hospital.
24	**Air Traffic Control -ATC (e.g. ENAV)**	Responsible for the provision of air traffic control service (ATCS), flight information service (FIS), aeronautical information service (AIS), and issuing of weather forecasts for the airports and the airspace under its responsibility.
25	**Interconnected / Interdependent Critical Infrastructures (e.g. metro/bus, refuelling corporation, hospitals, power/gas suppliers, communication suppliers)**	They activate their operational plans and act accordingly (usually if they face any cascade effect, or if they are needed to support the affected airport).
26	**Information Security Service Providers**	These services include Security Operation Centers (SOC), Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT).
27	**Telecommunications Providers**	National regulatory authority for the telecommunication.
28	**Airlines, Ground Handlers, Cargo**	**The Airline Operations and Control Centre** is an organizational unit of an airline. It hosts the roles of flight dispatch, slot management and strategic & CDM management, thereby managing the operations of the airline and implementing the flight programme. **The Ground Handling Agent** has the role to execute the aircraft turn-round agreements established with the aircraft operators and is responsible for the turn-round of all arriving aircraft. Ground handling covers a complex series of processes that are required to separate an aircraft from its load (passengers, baggage, cargo and mail) on arrival and combine it with its load prior to departure.
29	**Concessionaires**	Concession activities include for example car parking and rental, banking services and catering.
30	**Security and safety teams**	Members of these teams are responsible for protecting passengers, staff, aircraft, and airport property from accidental/malicious harm, crime, and other threats. Security and safety teams are experts on: (a) technical assets (e.g. gas, electricity, water), (b) hazardous materials (e.g. radioactive, etc.), human and material resources are combined in order to safeguard civil aviation against unlawful interference (such as terrorism, sabotage, threat to life and property, bombing, etc.). These teams are continuously trained and participate in tabletop and field exercises and simulations with passengers, staff, RFFS, volunteers etc.
31	**Passengers**	Customers of the airport, travel between the ground and air transportation modes or wait for a connection between two flights.

6.2 Holistic physical and cyber crisis management process

Crisis management has been defined as “the developed capability of an organization to prepare for, anticipate, respond to and recover from crises” (8). The airport’s crisis management process as well as the stakeholders involved in each phase (prepare, respond, recover and mitigate) are presented in the following subsections.

6.2.1 Preparedness phase

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions that internal and external stakeholders should follow closely in order to ensure organization readiness. In general, the following elements are crucial in preparing for crisis: i) the development of the Crisis Management Plan (CMP), ii) the identification of the critical assets and potential threats, iii) the clear structure, composition, and the specific roles assigned to the crisis management team and involved stakeholders, iv) the information management and the situational awareness among different stakeholders, v) the building of resilience by ensuring that all CMT members and stakeholders involved during the crisis management are suitably trained, vi) the affirmation that competent and adequate resources and equipment are available in order to perform the needed duties and vii) preparation of the communication strategy.

For an airport to prepare for crisis management, it is important to know which assets are vital for conducting its core activities, and which are the potential threats against these assets, as well as their vulnerabilities (step 1, see Figure 6.1). The ABoD, the DPO, the ADO, the physical security manager and personnel, the IT security manager and personnel, the technical manager and staff, and the IT department should cooperate and set in place the airport’s CMP. The methodology for the identification of critical assets, physical and cyber vulnerabilities, relevant effects should be defined by the IT department, the technical staff and the experts in the cyber and physical protection domain. The regulations, and best practices as documented and suggested by the external stakeholders (e.g. ICAO, EASA, National Civil Aviation Authority), the National Authorities (i.e. Ministry of Interior, Defence, Foreign Affairs, National Intelligence Agency, and National Data Protection Authority) should be taken into consideration and adopted. Additionally, the external stakeholders (i.e. safety and security teams, the airline operators, ground handlers and cargo, the telecommunication and post commission), should have their own emergency plans, which depending on the type of emergency might be activated and implemented.

Risk assessment constitutes the fundamental first step in preparedness and this means the identification and analysis of major threats, hazards and related vulnerabilities. This procedure helps organizations make decisions on equipment supply, maintenance and improvement, identification protective measures and to take quick decisions during the crisis.

Having determined the risks that could impact airports and how, actions that support response process should be identified. More specifically, appropriate institutional structures, clear mandates supported by comprehensive policies, plans and legislation and the allocation of resources for all these capacities through regular budgets are also instrumental for thorough preparedness to crisis.

The Crisis Management Plan (CMP) is a document that mostly sets out the following: i) persons in charge for key decisions and actions during a crisis, ii) the structure of the CMT (Crisis Management Team), and representatives involved in this team, iii) updated main contact list and the ways the communications will be held in the event of a crisis (including internal and external stakeholders), iv) the plans and mechanisms to be activated during a crisis and how they work in practice, v) flow charts specifying the sequence of actions and interactions and vi) definition of places for the CMT to meet, equipment and support required (57). Once the CMP has been written, approved and tested, airports should make sure to review and update it frequently and as part of the post incident review, as employees join or leave the company, new technologies are implemented, and other changes occur.

Currently, airports are responsible for the provision of the CMP, in accordance with the national and international laws and regulations, including:

- The international Standards and directives, NIS directive, ISO 27001, ISO 31000, ISO 27002.
- The National Civil Aviation Security Regulation and Security Technical Directives, which include information among other for the Airport Security measures, the Screening of Baggage, the Security equipment, etc.
- The recommended Practices of ICAO: Annex 14 "Aerodromes", Annex 18 "The Safe Transport of Dangerous goods by Air", Annex 11 "Air Traffic Services", Annex 9 "Facilitation", Annex 6 "Operation of Aircraft", Annex 17 "Operation of Aircraft".
- The EU Regulation 300/2008, laying down detailed measures for the implementation of the common basic standards on aviation security including information for the Access Control, the Screening of Persons, the Surveillance, Patrols and other Physical controls, etc.

Based on the level of the crisis, there exist several national CMPs, which might be activated. These plans and procedures are part of the regulatory framework that the airports follow. It is vital that all involved stakeholders understand their roles, and how the various plans are interconnected, in order to identify areas of potential improvements.

With regards to the **communication plans**, the airports should know what to communicate and to whom the information should be communicated. The type of crisis and its impacts set out the type of communication that is needed. During the crisis management phases, internal and external stakeholders should need different type of information for handling the incident.

In addition, to improve the efficiency of the CMT the appropriate tools must be in place (step 2, see Figure 6.1). The tools might include things from a contact list to hardware and software tools. The contact list includes contact details (e.g. address, telephone, email, back up contact info) of all those people that will help and collaborate during a crisis. Additionally, the CMT should make use of autonomous systems that can be used even when the organisation's systems or networks have been compromised. The internal and external stakeholders as identified in step 1 should use the appropriate tools that permit them to handle an incident.

Training and exercising are the cornerstones of preparedness which focus on readiness of all involved actors to respond to any type of incidents and emergencies and on the identification of any discrepancies in terms of resources (step 3). Most airports have dedicated structures for constant training of their staff. Training and exercising for crisis preparedness can focus on training units and individuals; testing equipment and the ability of staff to deploy and use it; controlling stocks of supplies; testing all components of contingency plans from the knowledge of the detailed protocols and procedures by the staff to the plan itself etc. Feedback from training can be used to enhance planning. All the internal stakeholders to be involved during the crisis management (see Table 6.1, No 1-13), and the external ones (see Table 6.2, No 14, 16-18, 21-23, 25, 26, 28, 30; e.g. law enforcement agencies, the RFFS, emergency medical services, interconnected critical infrastructures, security and safety teams), and airlines should regularly participate in the full and partial scale exercises, as well as in tabletop exercises (more than once per year). The ABoD should evaluate the effectiveness of the current Emergency Plan based on the exercise conclusions. The evaluation outcomes might lead to improvements that will be incorporated in the CMP.

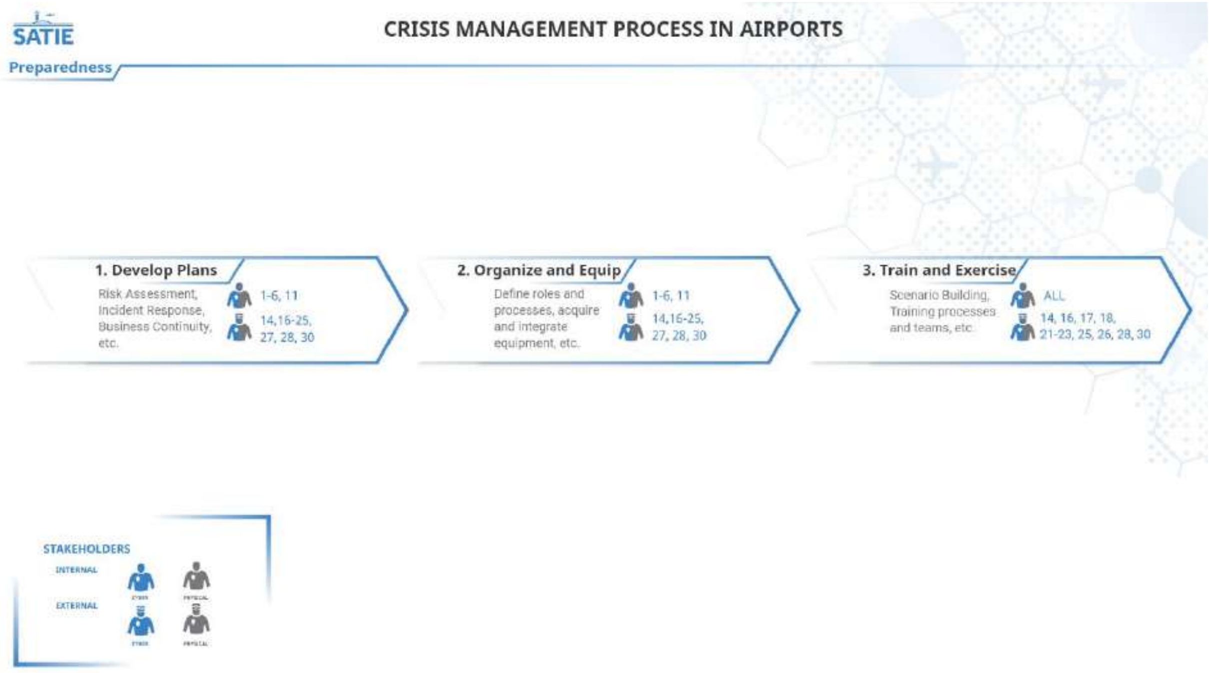


Figure 6.1: Preparedness phase

6.2.2 Response phase

Response initiates when an incident is detected by an internal stakeholder (or external stakeholder (e.g. SOC operated by an external organization) in a manual or automated way (e.g. monitoring networks and early-warning systems, public authorities, citizens, media, private sector, security personnel, etc.) (Step 4, see Figure 6.2). Involved stakeholders should start gathering information that will be used for the initial assessment of the incident. Depending on the type of the incident (cyber or physical or their combination) different stakeholders will collect the information needed for further investigations. Additionally, information from multiple sources, such as social media and crowdsourcing could be collected. The physical security manager, the IT security manager, and the technical manager should initiate the process. The SOC and the IT department, as well as the external stakeholders such as the law enforcement agencies, the RFFS, the interconnected critical infrastructures, the external security and safety teams, and the airlines and ground handlers could participate in this step. The information to be gathered usually includes details relevant to the type of incident, the present hazards, the access – routes that are safe to use, the number and the type of casualties (if any)[5], meteorological information, geolocation information, images, video, the timestamps, the analysis, the cause, the status, the custom parameters, etc. (step 5, Figure 6.2**)**. The information should be collected and assessed by the ADO in cooperation with relevant stakeholders that identified the incident (step 6, Figure 6.2**)**. Information gathering and assessment is a crucial and continuous step of this phase, as it highly depends not only on the source, quality, relevance of it, but also on the capacity of stakeholders involved in analysing, interpreting, understanding and adding value to raw information. Getting a clear picture of the crisis (e.g. what happened, how many people are or might be affected, issues, how the crisis might develop, what the means are in the operational field) is the basis for decision-making.

Based on the criticality of the incident, the Crisis or Emergency Management Team should be informed, triggered and coordinated by the Airport Duty Officer. The ADO with the support of the CMT should assess the extent of the crisis, evaluate the situation, determine, and define which

[5] https://jesip.org.uk/methane

response plan(s) should be activated (e.g. evacuation plan, etc.) and activate additional stakeholders to be involved, as deemed necessary. The ADO will also inform the ABoD, and the Media Centre (if needed). Depending on the stakeholders involved in the response phase (e.g. police, RFFS, etc.), different plans might be activated. Based on the activated plans, response processes and procedures are executed, co-ordinated and adapted. Disconnection, denial of remote access (i.e. VPN), isolation of affected systems, identification of root cause, and collection of logs could be some of the response actions to be followed (step 7, Figure 6.2**)**; appropriate resources should be allocated and released, and actions should be assigned to stakeholders and tracked by the ADO, with the support of the CMT or EOC in case that it has been activated by the ADO. Moreover, it is crucial to know the location of responders and their proximity to risks and hazards in real time, as well as to monitor and analyse passive and active threats and hazards at incident scenes in real time (58) (step 8, Figure 6.2**)**. In addition, the CMT is responsible for communicating in a timely, accurate and precise manner relevant information as collected in step 5 (that can be used for management, informative purposes), to internal and external stakeholders, in order to manage crisis and protect the brand and reputation of the organization by implementing relevant decisions (steps 9 & 10, Figure 6.2**)**. Leadership plays a key role in crisis communication. Communicating with the media and the general public to provide a sense of events, to maintain trust in the emergency responders and government, and to transmit specific messages are essential functions of leaders during crisis. Particular attention should be paid to the reports' circulating during a crisis handling. A great number of reports by the participants in the CMC agencies/organizations will be required by pertinent internal directives of these agencies or may be requested by senior management. The CMT usually maintains a log of the crisis and sets out the report after the crisis termination.

The afore-mentioned steps could repeat, until resources return to their original use and status (demobilization) and crisis terminates. As a crisis winds down, CMT should clearly indicate closure to the relevant internal and external stakeholders through a formal, well-communicated process to help minimise anxiety and encourage the return to normality. All the internal and external stakeholders that participated during the response phase participate in this step as well (step 11, Figure 6.2**)**.

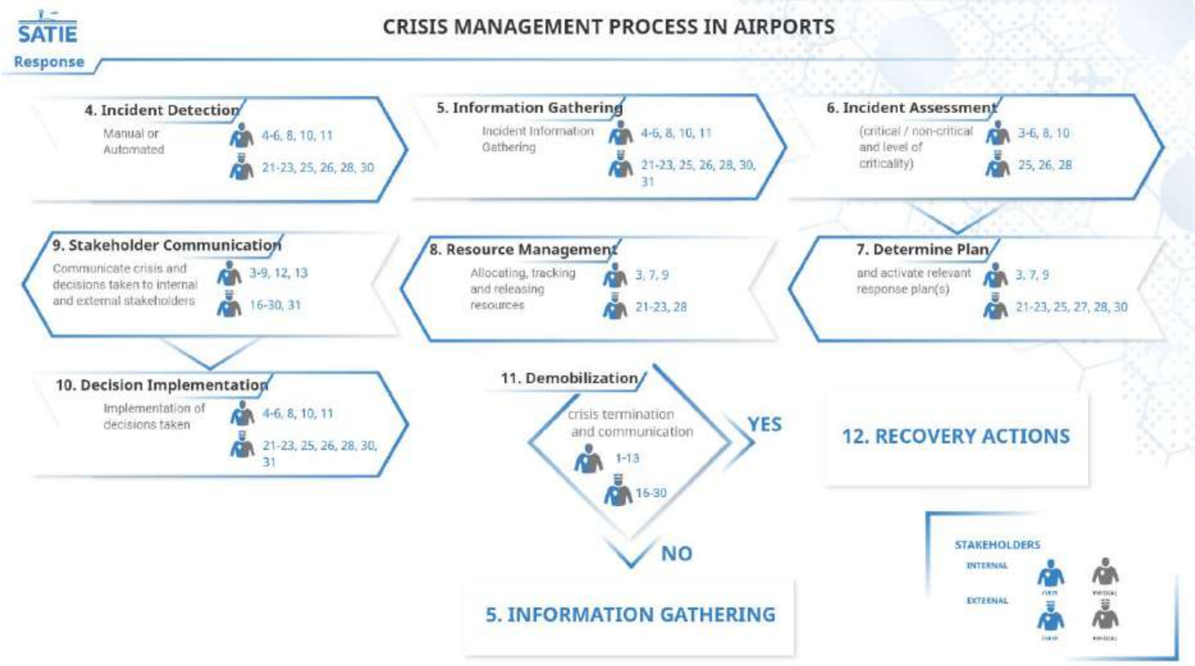


Figure 6.2: Response phase

6.2.3 Recovery phase

Recovery consists of those activities that continue beyond the emergency period to restore critical community functions and begin to manage stabilization efforts. This phase is executed during or after the response phase termination and is directly affected by decisions made as part of the previous phase. The CMT should decide the recovery actions to be taken (based on recovery plans), by coordinating closely with the ADO, the physical security manager and personnel, the IT security manager and personnel, the technical manager and staff, and the IT department in cooperation with external stakeholders (e.g. law enforcement agencies, RFFS, emergency medical services, interconnected critical infrastructures, third party providers, security and safety teams, and airlines) depending on the type of crisis and the activated response plans (step 12**,** Figure 6.3).

Airports should comply with the regulation (EC) No 300/2008 of the European Parliament and of the Council, ICAO annexes, along with nation-specific and airport-specific regulation which establish common rules in the European Union to protect civil aviation against acts of unlawful interference. With regards to cyber-attacks the following practices can help airports recover from them (as identified in chapter 5): i) remove infectious software and corrupt data permanently from systems that have been affected. The infectious software which might include malware, worms, and other forms of code that infiltrate a network should be removed permanently. In some cases, it is needed to isolate and then rebuild an infected system. This process is accomplished easier by using virtual machines; ii) recover data, software, or systems from archived backups, local configurations must be frequently backed up. The advantage of using virtual machines is that an entire image of a machine encompassing the operating system, software installed, and data can be quickly restored with little or no reconfiguration; iii) reauthorize access to data and systems. This procedure might include reinstating user access rights, reopening network communication ports and protocols; iv) reset credentials. If user access credentials are or are suspected of being lost, they should be reset so that new passwords and new user identifiers are issued and v) inform users that their data and systems have been recovered. With regards to physical attacks, on top of what the regulation (EC) No 300/2008 of the European Parliament and of the Council, the ICAO annexes, and the nation-specific and airport-specific regulations suggest, additional security measures are implemented by airports such as i) fences/walls, ii) guards, iii) building control, iv) intrusion detection and access control, v) video and audio surveillance systems, vi) Physical Security Information Management (PSIM) systems and vii) standardized screening techniques, which all passengers must undergo (e.g., baggage X-rays, metal detecting scans, shoe explosive detection systems, physical searches, detection dogs, etc., vii) security lighting, viii) pre-employment background checks, ix) aircraft security search or check, x) routine training and security awareness programs for the airport’s staff, etc.

Moreover, the evidence from the incidence should be collected by the ADO and CMT, in close cooperation with relevant internally involved stakeholders (e.g. the physical security manager and personnel, the IT security manager and personnel, the technical manager and staff, the IT department, AOC, EOC and SOC) and externally involved stakeholders (e.g. law enforcement agencies, RFFS, emergency medical services, interconnected critical infrastructures, third party providers, security and safety teams, and airlines), depending on the nature of the incident; analysed (step 13, Figure 6.3); and an evidence report should be created by CMT (step 14, Figure 6.3**)**. CMT in cooperation with ADO should share relative information with all internal stakeholders (step 15, Figure 6.3**)** and external stakeholders (e.g. AAIASB, CAA, GSCP, relative Ministries, LEAs, RFFS, emergency medical services, interconnected critical infrastructures, security and safety teams, and airlines) and investigations should be assisted (step 16, Figure 6.3). Moreover, as crisis serves as a major learning opportunity for both internal (e.g. ADO, CMT, physical and IT security managers and personnel, technical manager and staff, IT department) and external (e.g. AAIASB, LEAs, RFFS, emergency medical services, interconnected critical infrastructures, security and safety teams, and airlines) individuals and organizations, should review the overall process as well as plans, procedures, tools, facilities etc., to identify areas for improvement (step 17, Figure 6.3). Following the evaluation, lessons learnt should be identified (step 18, Figure 6.3) and recommendations / changes should be made to relevant plans and processes (step 19, Figure 6.3) by internal and external stakeholders (as described in step 1).

6.2.4 Mitigation phase

Lessons learned should be carried out for any crisis event. An airport or any type of organisation that has successfully been attacked should return to normal operations after new countermeasures have been implemented. Based on the outcomes of the incident consequences, some of the activities that previously were defined as normal will probably need to be revised. The results of the evaluation of the response actions should lead to recommendations for change, and responsibilities and timelines in order to ensure that it will be carried out (step 20, Figure 6.3). It is common, that discrepancies are identified but not actually addressed, resulting at the organization's disposal to future crises. Proposed changes might include organizational changes, structural (such as changing the characteristics of buildings; perimeter security etc.) and non-structural measures (adopting or changing physical and cyber access controls, training etc.). The ABoD, the DPO, the ADO, the physical security manager and personnel, the IT security manager and personnel, the technical manager and staff, and the IT department should get involved in the mitigation phase as deemed necessary. In this process, external stakeholders should get involved in setting or implementing the mitigation strategies, depending on the type of crisis and the evaluation of the response.

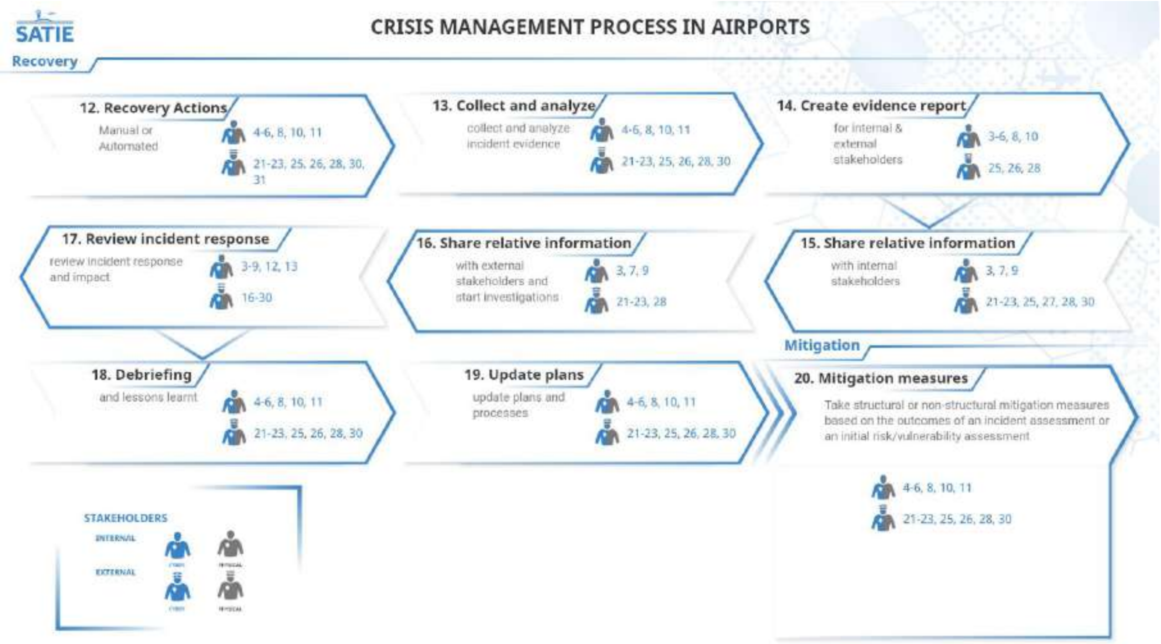

SATIE
CRISIS MANAGEMENT PROCESS IN AIRPORTS
Recovery
12. Recovery Actions
Manual or Automated
4-6, 8, 10, 11
21-23, 25, 26, 28, 30, 31
13. Collect and analyze
collect and analyze incident evidence
4-6, 8, 10, 11
21-23, 25, 26, 28, 30
14. Create evidence report
for internal & external stakeholders
3-6, 8, 10
25, 26, 28
15. Share relative information
with internal stakeholders
3, 7, 9
21-23, 25, 27, 28, 30
16. Share relative information
with external stakeholders and start investigations
3, 7, 9
21-23, 28
17. Review incident response
review incident response and impact
3-9, 12, 13
16-30
18. Debriefing
and lessons learnt
4-6, 8, 10, 11
21-23, 25, 26, 28, 30
19. Update plans
update plans and processes
4-6, 8, 10, 11
21-23, 25, 26, 28, 30
Mitigation
20. Mitigation measures
Take structural or non-structural mitigation measures based on the outcomes of an incident assessment or an initial risk/vulnerability assessment
4-6, 8, 10, 11
21-23, 25, 26, 28, 30
STAKEHOLDERS
INTERNAL
EXTERNAL

Figure 6.3: Recovery and mitigation phases

The following Figure 6.4, summarises the phases of the airport's crisis management process as well as the stakeholders involved in each phase, as already described in the previous paragraphs.

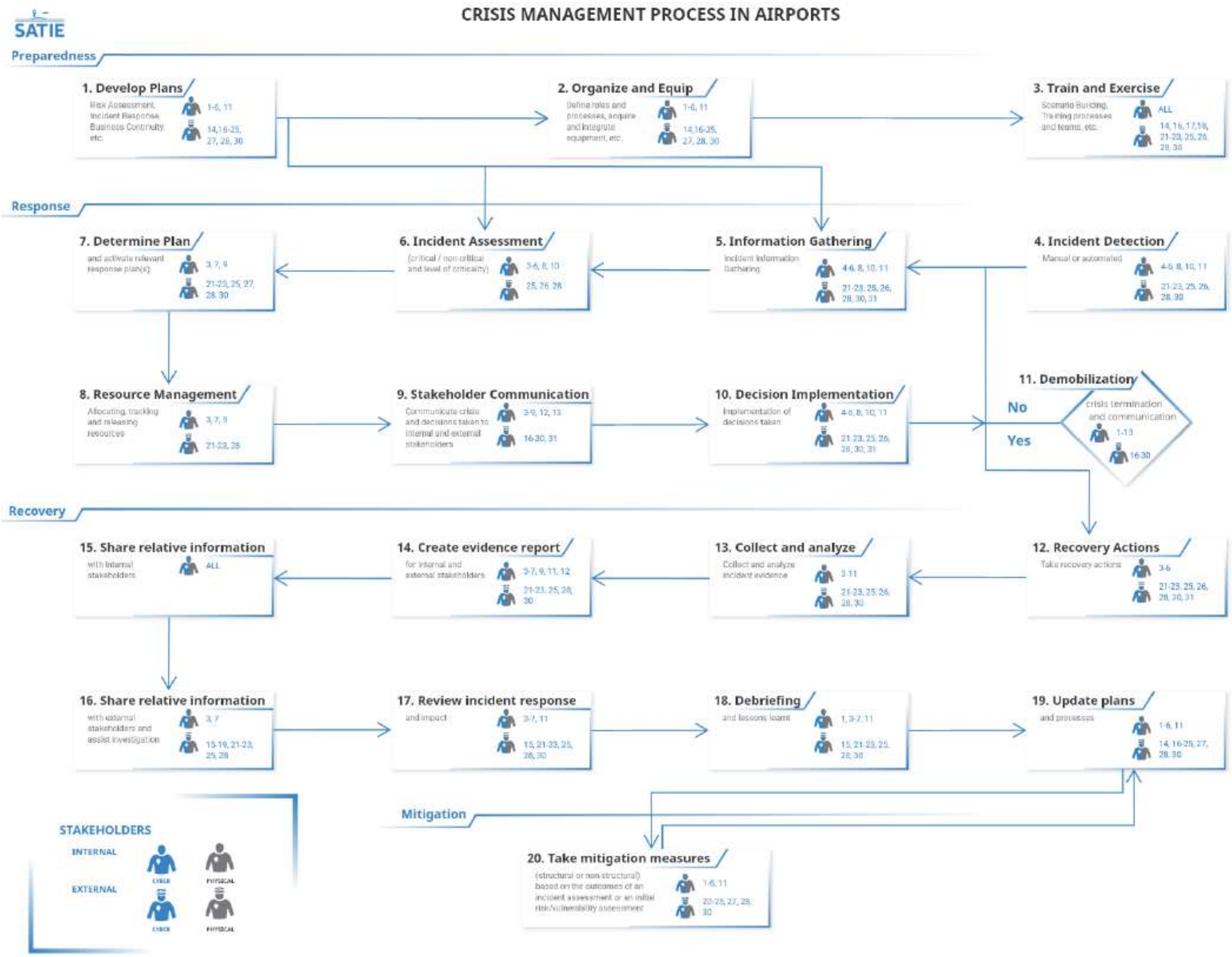

SATIE
CRISIS MANAGEMENT PROCESS IN AIRPORTS
Preparedness
1. Develop Plans
Risk Assessment, Incident Response, Business Continuity, etc.
1-6, 11
14,16-25, 27, 28, 30
2. Organize and Equip
Define roles and processes, acquire and integrate equipment, etc.
1-6, 11
14,16-25, 27, 28, 30
3. Train and Exercise
Scenario Building, Training processes and teams, etc.
ALL
14, 16, 17,18, 21-23, 25, 26, 28, 30
Response
7. Determine Plan
and activate relevant response plan(s)
3, 7, 9
21-23, 25, 27, 28, 30
6. Incident Assessment
(critical / non-critical and level of criticality)
3-6, 8, 10
25, 26, 28
5. Information Gathering
Incident Information Gathering
4-6, 8, 10, 11
21-23, 25, 26, 28, 30, 31
4. Incident Detection
Manual or automated
4-6, 8, 10, 11
21-23, 25, 26, 28, 30
8. Resource Management
Allocating, tracking and releasing resources
3, 7, 9
21-23, 28
9. Stakeholder Communication
Communicate crisis and decisions taken to internal and external stakeholders
3-9, 12, 13
16-30, 31
10. Decision Implementation
Implementation of decisions taken
4-6, 8, 10, 11
21-23, 25, 26, 28, 30, 31
11. Demobilization
No
Yes
crisis termination and communication
1-13
16-30
Recovery
15. Share relative information
with internal stakeholders
ALL
14. Create evidence report
for internal and external stakeholders
3-7, 9, 11, 12
21-23, 25, 28, 30
13. Collect and analyze
Collect and analyze incident evidence
3-11
21-23, 25, 26, 28, 30
12. Recovery Actions
Take recovery actions
3-6
21-23, 25, 26, 28, 30, 31
16. Share relative information
with external stakeholders and assist investigation
3, 7
15-19, 21-23, 25, 28
17. Review incident response
and impact
3-7, 11
15, 21-23, 25, 28, 30
18. Debriefing
and lessons learnt
1, 3-7, 11
15, 21-23, 25, 28, 30
19. Update plans
and processes
1-6, 11
14, 16-25, 27, 28, 30
Mitigation
20. Take mitigation measures
(structural or non-structural) based on the outcomes of an incident assessment or an initial risk/vulnerability assessment
1-6, 11
20-25, 27, 28, 30
STAKEHOLDERS
INTERNAL
EXTERNAL
CYBER
PHYSICAL
CYBER
PHYSICAL

Figure 6.4: Common and holistic security and safety agenda

7 Conclusions

Current deliverable focused on the presentation of the holistic crisis management cycle in the context of airports. In this respect, the cyber and physical rules and policies that are relevant to the project's needs have been presented, the security and safety procedures per each airport and SATIE scenario have been described (intentionally not included in this report), the different stakeholders as well as the main operations executed by the AOC and the various activities coordinated by the AOC have been highlighted.

The provided information led to the identification of the holistic airports' crisis management cycle including the relevant stakeholders and processes. Taking into consideration the findings from SATIE workshops, reports of major national emergencies and disasters, and the daily challenges faced by the airports, areas for improvement have been identified. In this regard, the holistic security/safety agenda being ultimately proposed by SATIE provides for setting the common ground among all stakeholders in managing a crisis thus reducing administration/coordination overhead and enhancing the process of efficient decision making.

As it has been highlighted, during a cyber and/or physical incident, different categories of stakeholders either internal or external might be fundamentally affected when an airport's routine operations are compromised and disrupted. The crisis management is an extensive procedure, and the interactions among the numerous stakeholders can be very complex. Situational awareness and information sharing have been recognized as a critical foundation for successful incident response and decision-making activities during the crisis management process. SATIE adopts a holistic approach by developing an interoperable toolkit that improves situational awareness at airports and cooperation among different stakeholders. Having a shared situational awareness, the various stakeholders involved in the crisis management collaborate more efficiently to the crisis resolution. Emergency procedures can be triggered simultaneously through an alerting system in order to reschedule operations, notify stakeholders including first responders, cyber/physical security and maintenance teams towards a fast and effective response and recovery.

8 References

1. *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* **Izuakor C., White R.** United States : s.n., 2016 . 10th International Conference on Critical Infrastructure Protection (ICCIP). pp. 27-41.

2. **European Commission.** *Communication from the Commission on a European Programme for Critical Infrastructure Protection,.* Brussels : s.n., 2006.

3. **Commission, European.** *Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection.* Brussels : s.n., 2008.

4. —. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* 2009.

5. **SESAR.** *Periodic Reporting for period 2 - PJ04 TAM (Total Airport Management).* 2018.

6. **Kanyi, P.M., Kamau, P.K. and Mireri, C.** Assessment of the appropriateness and adequacy of the existing physical infrastructure in mitigating aviation risks at Wilson Airport, Kenya. *IOSR J. Humanit. Social. Sci.* 21, 2016, pp. 51-62.

7. **Levent Kenar, Turan, K.; Mehmet, E.; Mesut, O.; Hakan, Y.** Chemical release at the airport and lessons learned from the medical perspective. *J. Hazard. Mater.* 2007, Vol. 144, pp. 396–399.

8. **British Standard Institute (BSI).** *BS11200: Crisis Management – guidance and good practice .* s.l. : BSI, 2014.

9. **Zografos, K.; Madas, M.; Salouras, Y.** A decision support system for total airport operations management and planning. *J. Adv. Transp.* 47, 2013, pp. 170–189.

10. **Sunkyung, C.; Shinya, H.** Estimating the mean waiting time in airports through cooperative disaster response operations. J. Air Transp. Manag, 2017, pp. 11-17.

11. **Stanley, L.; Harriman, O.; Fanjoy, A.; Petrin, 0.** Small general aviation Airport emergency Preparedness and the perceived risks of very light jet operations. *J. Aviat./Aerosp. Educ. Res.* 19, 2009.

12. **Stephanie, C.; Ericson, E.; Laurie, D.** *Airport Closures in Natural and Human-Induced Disasters, Business Vulnerability and Planning.* Ottawa : s.n., 2003.

13. **Airport Cooperative Research Program (ACRP).** Airport Cooperative Research Program (ACRP). [Online] 2019. http://www.trb.org/Publications/PubsACRPProjectReports.aspx.

14. *Planning and preparing for public health threats at airports.* **Martin, Greg & Boland, Mairin.** 2018, Globalization and Health.

15. *Airport Disaster Preparedness in a community context.* **James F. Smith.** 2009.

16. *Effective Cooperation Among Airports and Local and Regional Emergency Management Agencies for Disaster Preparedness and Response.* **National Academies of Sciences, Engineering, and Medicine.** 2014, Washington, DC: The National Academies Press. https://doi.org.

17. *Emergency Guidebook for General Aviation Airports.* **Airport Assistance Program.** 2008.

18. **National Academies of Sciences, Engineering, and Medicine.** *Guidebook on Best Practices for Airport Cybersecurity.* s.l. : Best Practices for Airport Cybersecurity. Washington, DC: The National, 2015.

19. **Deloitte.** Cyber crisis management: Readiness, response, and recovery. *Deloitte.* [Online] 2016. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=16&cad=rja&uact=8&ved=2ahUKEwij0amRn_3lAhXISxUIHeu5AWAQFjAPegQICRAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fde%2FDocuments%2Frisk%2FDeloitte-Cyber-crisis-management-Rea.

20. **National Academies of Sciences, Engineering, and Medicine.** *Airport Emergency Post-Event Recovery Practices.* 2015.

21. **ENISA.** *Securing Smart Airports.* 2016.

22. **ACRP.** *Information Technology Systems at Airports.* s.l. : ACRP, 2012.

23. **Satzinger, John W.** *Systems Analysis and Design in a Changing World.* 2011.

24. **Price, Jeffrey.** *Practical Airport Operations, Safety, and Emergency Management: Protocols for Today and the Future.* s.l. : Butterworth-Heinemann, 2016.

25. *Security Operation Center Concepts & Implementation.* **Bidou, Renaud.** 2005.

26. **Fraport.** *Integrated Airport Operations.* [Online] 2018. https://www.fraport.com/content/fraport/en/business-partner/consulting-training/consulting/integrated-airport-operations.html.

27. **SESAR.** *SESAR 2020 Concept of Operations Edition.* 2017.

28. **EUROCONTROL.** *Airport Network Integration. Concept for establishment of an Airport Operations Plan (AOP).* 2018.

29. **Günther, Yves & Inard, Anthony & Werther, Bernd & Bonnier, Marc & Spies, Gunnar & Marsden, Alan & Temme, Marco-Michael & Böhme, Dietmar & Lane, Roger & Niederstraßer, Helmut.** *Total Airport Management (Operational Concept and Logical Architecture).* 2006.

30. **ICAO.** *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference.* [Online] https://www.icao.int/Security/Pages/default.aspx.

31. **Alliance, National Safe Skies.** *PARAS. Recommended Security Guidelines for Airport Planning, Design, and Construction.* s.l. : National Safe Skies Alliance, Inc. Sponsored by the Federal Aviation Administration, 2017.

32. **Hutter, David.** *The Importance of Physical Security.* s.l. : The SANS Institute, 2016.

33. **PARAS.** *Airport Perimeter Breach Classification and Post-Incident Best Practices.* s.l. : National Safe Skies Alliance, Inc., 2016.

34. **Hutter, David.** *Physical Security and Why It Is Important.* s.l. : SANS Institute. Physical Security and Why It Is Important., 2016.

35. **DRIVER project.** [Online] 2014. https://www.driver-project.eu/.

36. **Raytheon.** [Online] 2019. https://www.raytheon.com/news/feature/cyber_secure_aviation.

37. **Pasztor, Andy.** Aviation Industry Seeks to Strengthen Cybersecurity Defenses . *Wall Street Journal.* [Online] 2017. https://www.wsj.com/articles/aviation-industry-seeks-to-strengthen-cybersecurity-defenses-1498104452.

38. *Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls.* **Lykou, G., Anagnostopoulou, A., Gritzalis, D.** 2019, Sensors.

39. **ICAO.** *RESOLUTIONS ADOPTED AT THE 39TH SESSION OF THE ASSEMBLY.* [Online] 2016. https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf.

40. *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond.* **Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C.** s.l. : IEEE, 2011. Proceedings of the IEEE. pp. 2040-2050.

41. *Proposal Security Solutions to Protect Automation System from Denial of Service in Airports.* **Afify, F., Badawy M.** 2014, International Journal of Scientific and Engineering Research.

42. **Delain O., Ruhlmann O., Vautier E.** *Addressing Airport Cyber- Security.* [Online] 2016. https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf.

43. **ACI, Airports Council International.** [Online] 2019. https://aci.aero/news/2019/09/04/aci-world-launches-new-guidance-on-airport-business-continuity-management/.

44. **27001:2013, ISO/IEC.** Information technology — Security techniques — Information security management systems — Requirements. [Online] International Organization for Standardization, 2013. [Cited: 10 21, 2019.] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

45. **31000:2018, ISO.** *Risk management — Guidelines.* s.l. : International Organization for Standardization (ISO).

46. **ISO/IEC, 27005:2018.** Information technology — Security techniques — Information security risk management. [Online] International Organization for Standardization, 2018. https://www.iso.org/standard/75281.html.

47. **27033:2015, ISO/IEC.** *Information technology — Security techniques — Network security.* [Online] International Organization for Standardization, 2015. https://www.iso27001security.com/html/27033.html.

48. **22301:2012, ISO.** Societal security — Business continuity management systems — Requirements. *ISO 22301.* [Online] https://www.iso.org/standard/50038.html.

49. **27002:2013, ISO/IEC.** *Information technology — Security techniques — Code of practice for information security controls.* [Online] International Organization for Standardization, 2013. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

50. **EU NIS Directive 2016/1148.** [Online] ENISA, 2016. https://www.enisa.europa.eu/topics/nis-directive.

51. **EASA.** Standards on cybersecurity, an aviation framework. [Online] https://www.sae.org/binaries/content/assets/cm/content/attend/2017/aerospace-standards-summit/standards_on_cybersecurity.pdf.

52. **United Nations Office for Disaster Risk Reduction.** Terminology on Disaster Risk Reduction. [Online] 2017. https://www.unisdr.org/we/inform/terminology.

53. **Thoma, Klaus.** *Resilience by Design: a strategy for technology issues of the future.* s.l. : acatech, National academy of science and engineering, 2014.

54. **Woods, David D.** Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety 141.* 2015, pp. 5-9.

55. **Häring, Ivo, et al.** Towards a Generic Resilience Management Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies. *Resilience and risk.* s.l. : Springer Dordrecht, 2017, pp. 21-80.

56. **International Organization for Standardization.** ISO 31000 Risk management. Genf : s.n., 2018.

57. **AIRPORT COOPERATIVE RESEARCH, PUBLICATION.** *Emergency Communications Planning for Airports.* 2016.

58. **Homeland Security Studies and Analysis Institute.** *2014 National Technology Plan for Emergency Response to Catastrophic Incidents.* s.l. : Homeland Security, 2014.

59. **SATIE project.** *DX.X - name of the SATIE deliverable you want to reference.* 2019.

60. **Sunkyung C., Shinya H.** Diagramming development for a base camp and staging area in a humanitarian logistics base airport. *J. Humanit. Logist - Supply Chain Manag.* 2017, Vol. 7, pp. 152-171.

61. **Abdussamet, Polater, et al.** Managing airports in non-aviation related disasters: A systematic literature Review. *International Journal of Disaster Risk Reduction.* 2018, Vol. 31, pp. 367-380.

62. *Now That's Smart!* **Vyatkin, Valeriy, et al.** Issue: 4 , Valeriy et al 07 : IEEE Industrial Electronics Magazine, 2007, Vol. Volume: 1 . 17-29.

63. **Comission, EU.** *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (.* 2017.

64. **Fachiot.** *Aviation safety requires a holistic, systems-based approach.* 2018.

65. **Flight Safety Foundation.** [Online] 2017. https://flightsafety.org/easa-initiates-aviation-cyber-security-program/.

66. **EASA.** [Online] 2019. https://www.easa.europa.eu/eccsa.

67. *Risk Assessment Procedure for Civil Arport .* **Distefano, Natalia.** 2013, ijtte.

68. **ACRP.** *A Guidebook for Safety Risk Management for Airports.* 2015.

69. **Kolesar, Jan.** *Risk Management in the sphere of Civil Airport Protection against unlawfull interference.* 2012.

70. **Haselton, Todd.** A Look Inside AT&T's Global Network Operations Center (GNOC). [Online] 2012. https://www.technobuffalo.com/a-look-inside-atts-global-network-operations-center-gnoc.

71. **Fraport.** *Integrated Airport Operations.*

72. **Pujet, Nicolas.** *Modeling and Arline Operations Control.* 1998.

73. **National Academies of Sciences Engineering and Medicine.** *Emergency Communications Planning for Airports.* s.l. : The National Academies Press, 2016.

74. *A taxonomy of situation awareness errors, human factors in aviation operations. .* **Endsley, M.** 1995. 21st Conference of the European Association for Aviation Psychology (EAAP). pp. 287-292.

75. **ISA/IEC 62443.** *security capabilities for control system components.* [Online] 2018. https://www.isa.org/intech/201810standards.

76. **EURACTIV.** [Online] 2019. https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/.

77. **SkyBray.** [Online] 2019. https://www.skybrary.aero/index.php/Safety_Management.

78. **ACI.** [Online] 2019. https://aci.aero/about-aci/priorities/safety/sms/.

79. **Fireside.** [Online] 2019. https://www.firesideteam.com/pages/emergency-operations-center-1.