This project has received funding
from the European Union's Horizon Europe Programme

RESEARCH PROJECT EASA.2022.HVP.04

VERIFICATION OF SECURITY-RELATED REQUIREMENTS DURING CERTIFICATION PROCESSES (GAP ANALYSIS AND BEST PRACTICES)

D-3.2.2

Impact of Security Measures on Safety

Research conducted by:

UK Civil Aviation Authority International

apave Aeroservices

CASRA

Disclaimer

This study has been carried out for EASA by consortium lead CAA International (CAAi) upon award of a specific contract for the provision of consultancy services. Consequently, it does not necessarily express the views of EASA itself, nor should it be relied upon as a statement, as any form of warranty, representation, undertaking, contractual, or other binding commitment upon EASA. Ownership of all copyright and other IPR in this material including any documentation, data, and technical information, remains vested to EASA. All logos, copyrights, trademarks, that may be contained within, are the property of their respective owners. Reproduction of this study, in whole or in part, is permitted under the condition that this Disclaimer remains clearly and visibly affixed in full at all times with such reproduced part.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Union Aviation Safety Agency (EASA). Neither the European Union nor EASA can be held responsible for them.

This deliverable has been carried out for EASA by an external organisation and expresses the opinion of the organisation undertaking this deliverable. It is provided for information purposes. Consequently, it should not be relied upon as a statement, as any form of warranty, representation, undertaking, contractual, or other commitment binding in law upon the EASA.

Ownership of all copyright and other intellectual property rights in this material including any documentation, data and technical information, remains vested to the European Union Aviation Safety Agency. All logos, copyrights, trademarks, and registered trademarks that may be contained within are the property of their respective owners. For any use or reproduction of photos or other material that is not under the copyright of EASA, permission must be sought directly from the copyright holders.

No part of this deliverable may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner. Should the owner agree as mentioned, then reproduction of this deliverable, in whole or in part, is permitted under the condition that the full body of this Disclaimer remains clearly and visibly affixed at all times with such reproduced part.

DELIVERABLE NUMBER AND TITLE:	[Verification of security-related requirements during certification processes (gap analysis and best practices) – D-3.2.2]
CONTRACT NUMBER:	EASA.2022.HVP.04
CONTRACTOR / AUTHOR:	CASRA / Cédric Lüthi (Task Leader) – Adam Troczyński (Co-author) – Céline Delay (Co-author)
IPR OWNER:	European Union Aviation Safety Agency
DISTRIBUTION:	[Public]

APPROVED BY:	AUTHOR	REVIEWER	MANAGING DEPARTMENT
	CASRA / Adam Troczyński CASRA / Céline Delay	CASRA / Cédric Lüthi UK CAA Apave	CASRA

DATE: 27/02/2025

CAA International Limited (CAAi) was established in April 2007 as a wholly owned subsidiary of the UK CAA. The UK Civil Aviation Authority (UK CAA) is the UK's specialist aviation regulator, directly reporting to the UK Government's Department for Transport (DfT). Through its skills and expertise, it is recognised as a world leader in its field. CAAi provides access to the UK CAA's wealth of expertise and experience within the five operating groups of the UK CAA (Safety & Airspace Regulation Group, Consumers and Markets Group, Security Group, Strategy and Policy Group and International Group). Its primary focus is providing advisory, training, examination and licencing services to agencies, fellow National Aviation Authorities and industry in over 140 countries. CAAi's work involves assessment and delivery of targeted safety, security and environmental improvements and offer unparalleled expertise stemming from insights into best practices defined by the CAA.

Apave's core business is to help companies and government services managing their technical, environmental and human risks in the areas of Oil & Gas / Nuclear / Industry / Transportation. In aviation, Apave is committed to offering a range of civil and military aviation safety services, covering oversight authority tasks, audits, technical control, training and consulting services, through specialised and dedicated entities. Apave's staff in aviation enjoy extensive knowledge of the International and European regulatory framework, with a focus on Airworthiness, Flight Operations and Safety Management Systems In 2022 Apave has strengthened its portfolio through the acquisition of Oppida a cyber-security specialist in many highly regulated domains and safety and security exposed businesses. Apave has organised its civil and military aviation risk management consulting services around a unique value proposition with a dedicated entity: Apave Aeroservices (hereafter referred to as ''Apave") has been designated in 2009 as the Group centre of excellence to provide risk management solutions to the Aviation community, including aviation authorities, Air Operators, Industry, Maintenance Organisations (MROs - Maintenance, Repair & Overhaul) and Training Organisations.

APSS Software & Services Ltd is part of the Centre for Adaptive Security Research and Applications (CASRA), which was founded in 2008. CASRA emerged from the Visual Cognition Research Group of the University of Zurich, which was founded by Adrian Schwaninger in 1999. Today, CASRA APSS has a workforce of around 35 people, comprising of psychologists, economists, computer scientists, imaging specialists, software developers, aviation security experts, and more, most of which have an academic degree. The main objective of CASRA is to increase security and facilitation at airports and other environments involving people and technology. Through their studies and research on human – machine interaction, it was identified that visual abilities and training determine largely screeners' performance. As such CASRA has been working with a number of aviation security authorities and airports on selection, training and competency assessment processes providing advisory and research as well as their solutions globally.

TABLE OF CONTENTS

Abbreviations 6

1. Executive summary 7

2. Introduction 9

2.1. Context and background 9

2.2. Objectives of the document 9

3. Methodology 15

3.1. Survey 16

3.2. Interviews 17

3.2.1. Interview guide 18

4. Results 20

4.1. Survey 20

4.1.1. Initial contact 21

4.1.2. Security program submission 21

4.1.3. Document evaluation phase 21

4.1.4. On-site inspection phase 22

4.1.5. Audit Outcome 22

4.1.6. Post-certification oversight 23

4.1.7. Post-issuance phase 23

4.2. Interviews 23

4.2.1. Security consideration in certification 25

4.2.2. Desired security requirements in certification 26

4.2.3. Preferred certification audit approach 26

4.2.4. Challenges in managing safety and security 27

4.2.5. Personnel familiarity with safety and security 27

4.2.6. Safety and security process alignment 28

5. Discussion 29

5.1. Aerodromes certification 29

5.2. Air Operators certification 36

5.3. Gaps 41

5.4. Best practices 43

6. Conclusion 44

Bibliography 46

Appendix 47

Interview answers covering aerodromes certification 47
Interview answers covering air operator’s certification 50

ABBREVIATIONS

ACRONYM	DESCRIPTION
AA	Appropriate Authority
AM	Aerodrome Manual
AOSP	Air Operator Security Program
AOC	Air Operator Certificate
CA	Competent Authority
CAT	Commercial Air Transport
EASA	European Union Aviation Safety Agency
EC	European Commission
EEA	European Economic Area
EU	European Union
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IOSA	IATA Operational Safety Audit
NAA	National Aviation Authority
NCASP	National Civil Aviation Security Program
OM	Operations Manual
SMS	Safety Management System
SeMS	Security Management System
CAME	Continuing Airworthiness Management Exposition
CM	Compliance Manual
AMC	Acceptable Means of Compliance
CCTV	Closed-circuit television

1. Executive summary

Problem area

The general objective of the project *Impact of security measures on safety* is to understand the nature and extent of interdependencies between safety and security. Through the research within this project, an attempt is made to produce the comprehensive knowledge base describing these interdependencies.

Task 3 focuses on the analysis of certification standards with subtask 3.2 assessing the impact of security-related requirements on the safety certification and/or licensing of air operators and aerodromes.

Executive Summary

This report represents deliverable D-3.2.2 of Task 3: "*Verification of security-related requirements during certification processes (gap analysis and best practices)*," focusing on the analysis and evaluation of security requirements within the certification processes for aerodromes and air operators implemented through Competent Authorities (CAs) in accordance with the European Union (EU) regulations. **The primary goal of this document is to determine if, how, and to what extent security requirements are assessed during these certification processes.**

The report delves into the regulatory framework governing aerodrome and air operator certifications across EU/European Economic Area (EEA) states, explores the distribution of competencies at the national level, including the relationships and processes between safety (Competent Authority) and security (Appropriate Authority) authorities. It assesses the relationships between the certification processes and security requirements' conformity, and examines the interdependencies, overlaps, and differences, and if these lead to the potential gaps or can support development of best practices. The research activities for this report were grounded in extensive stakeholder engagement, encompassing perspectives from representatives of authorities, airport operators and air operators (in the form of surveys and interviews).

The report concludes that CAs adhere to the certification framework established by European Union Aviation Safety Agency (EASA) rules and, in some cases, have developed separate security certifications to complement safety certifications. While interdependencies between safety and security are generally well understood, certain areas require enhanced coordination to address overlapping or mutually impacting requirements.

Key findings presented in this report indicate that the certification processes for aerodromes and air operators (referred to as safety certification) are well-established and implemented consistently across the EU by CAs. These processes, conducted by safety domain experts, ensure comprehensive verification of conformity with certification requirements. Coordination and collaboration mechanisms between safety and security domains are in place.

The research confirmed security elements included in the certification framework are generally integrated into safety certification processes, however, they are rather limited. While CAs aim at assurance that certification requirements are adhered to, variations in detailed implementation exist. This includes instances where states develop separate security certifications alongside safety certifications for aerodromes (airports) and air operators extending the scope of such certification to conformity with aviation security common standards not included in the EU certification requirements.

In terms of interdependencies and coordination stakeholders generally recognise relationships between safety and security. Collaboration and coordination mechanisms have been established to facilitate information exchange and ensure that security requirements are adequately assessed during certification processes.

Security requirements are more frequently assessed in air operator certifications and have more impact on the result of the certification compared to aerodrome certifications.

With regards to challenges and recommendations the overall assessment indicates that **while safety and security domains can operate rather independently, improved coordination and integration processes are recommended for overlapping areas** and in terms of the organisation of management of entities.

It has been also noted through the study that the expertise required in safety and security differs significantly, necessitating an adequate pool of human resources and close collaboration between domain experts to ensure synchronised processes and promoting cross-domain integration to address areas where safety and security intersect. Safety authorities also often lack access to details of specific security requirements due to confidentiality, increasing reliance on security experts. Enhancing information-sharing practices to overcome these confidentiality barriers would be desirable.

Finally, certification requirements referencing security elements should be streamlined, clarified, and updated. Additional guidance is recommended to facilitate a more comprehensive assessment of security elements in the certification processes, including relevance of security requirements in the certification process or aerodromes and air operators. Developing additional guidance to clarify security-related certification requirements could be helpful in this process.

The analysis and discussion presented in this document provide a valuable resource for understanding the correlations between safety and security in the certification processes of aerodromes and air operators. By addressing existing gaps and identifying best practices, the findings offer a pathway for more robust and harmonized certification processes across EU/EEA states.

This report serves as a foundational step toward achieving greater integration and coherence between safety and security domains, ensuring the continued safety and security of aviation operations.

2. Introduction

This chapter first provides the context and background of the project (Section 2.1) and then objectives of the document are presented (Section 2.2).

2.1. Context and background

The European Union Aviation Safety Agency (hereinafter "EASA") is an agency of the European Union, which has been given specific regulatory and executive tasks in the field of aviation safety. The Agency constitutes a key part of the European Union's strategy to establish and maintain a high uniform standard of safety and environmental protection in civil aviation at European level.

As part of the Horizon Europe Work Programme 2021-2022 on Cluster 5 Climate, Energy and Mobility, the European Commission has entrusted EASA with the management of one specific research action entitled "Impact of security measures on safety".

As a result, EASA has awarded a public contract to a consortium of three companies:

- CAA International
- Apave Aeroservices
- CASRA

The contract details the four main tasks which are specified in order to achieve the expected outcome which is to understand the nature and extent of the interdependencies between safety and security in order to assess the impact of security measures on safety. In doing so, the research project should identify which processes and job roles are affected by safety–security interdependencies and which certification requirements and licensing activities are affected. In the medium term, safety risk management techniques that can be applied to security will produce harmonised risk assessment methods and support integrated policy and decision-making processes at national and EU level.

The project aims at developing a comprehensive knowledge base for the evaluation of the potential impact of security measures on the safety performances of aviation systems, personnel and operations, including the leading indicators for measuring such an impact (positive or negative) as well as the main factors playing a role in such safety - security dependencies.

The four main tasks are:

- Task 1: Identify the interdependencies between security and safety
- Task 2: Assessment of the impact of security measures on safety
- Task 3: Analysis of certification standards
- Task 4: Integrated risk management

The intention of this activity is to provide a basis for better understanding of where security threats have safety consequences in a more granular way than is currently understood.

2.2. Objectives of the document

Task 3 covers the analysis of certification standards in the context of safety-security interdependencies and the assessment of the impact of security measures on safety.

Subtask 3.2 focuses on the assessment of the impact of security-related requirements in the safety certification air operators and aerodromes.

The present report is the deliverable D-3.2.2 of task 3: "*Verification of security-related requirements during certification processes (gap analysis and best practices)*".

The certification of air operators and aerodromes shall ensure that only entities that demonstrate compliance with the applicable requirements are allowed to provide regulated services. From the regulatory perspective the certification is the responsibility of the CAs, therefore this report focuses on an assessment performed by this authority. The research acknowledged that security is the domain of the Appropriate Authority (AA) which in the majority of assessed cases is the same as CAs.

The objective of this document was to investigate how these certification processes implemented by CAs work in different EU/EEA countries:

- What are similarities? What are differences?
- What recommendations and best practices can be formulated?

The research was conducted in two main steps: first, a survey to provide a general overview of how the certification processes work, followed by interviews for deeper insights.

This report follows deliverable D-3.2.1 that investigated and elaborated on the overarching certification process framework applicable to aerodromes and air operators according to EU requirements and regulations and based on national implementation. D-3.2.1 equally acknowledged that there is no formal EU security certification of aerodromes and air operators however the certification process is defined in EU aviation security regulations for some other elements[1].

Table 1 summarises key regulatory aspects concerning aviation safety and security.

Table 1: Key aspects concerning aviation safety and security regulatory system in the EU

Aspect	Aviation Safety	Aviation Security
Primary focus	Ensuring safety by managing safety hazards leading to accidents and incidents	Ensuring security by prevention of intentional acts leading to acts of unlawful interference endangering safety
Key EU Regulations	Regulation (EU) No 2018/1139 and related acts	Regulation (EC) No 300/2008 and related acts
Main EU Regulator	European Union Aviation Safety Agency (EASA)	Directorate-General for Migration and Home Affairs (DG HOME)
National Authorities	National Aviation Authority (NAA) / Competent Authority (CA)	Appropriate Authority (AA)
Key Responsible Roles in regulated entities	Accountable Manager Nominated Persons (Postholders)	Security Manager(s)

[1] See Section 7 "Security Certification" of the D-3.2.1 Assessment report on existing safety and security certification requirements.

Aspect	Aviation Safety	Aviation Security
Standards & Procedures	Established through set of mandatory manuals (originating from Aerodrome Manual and Operations Manual)	Established by the mandatory security programs (Airport Security Program and Air Operator Security Program)
Training Requirements	Initial and recurrent trainings based on roles	Initial and recurrent training based on roles
Risk Assessment	Required as part of the Safety Management System (SMS) from aerodromes and air operators	Required as per National Civil Aviation Security Program of each state (no overall recognition of SeMS)
Compliance & Enforcement	Ensured by internal compliance monitoring, national oversight and EASA	Ensured by internal quality control, national oversight and DG MOVE

Figure 1 and Figure 2 below provide a concise overview of the aerodrome and air operator certification process respectively, consisting of phases that follow the International Civil Aviation Organization (ICAO) model.[2]

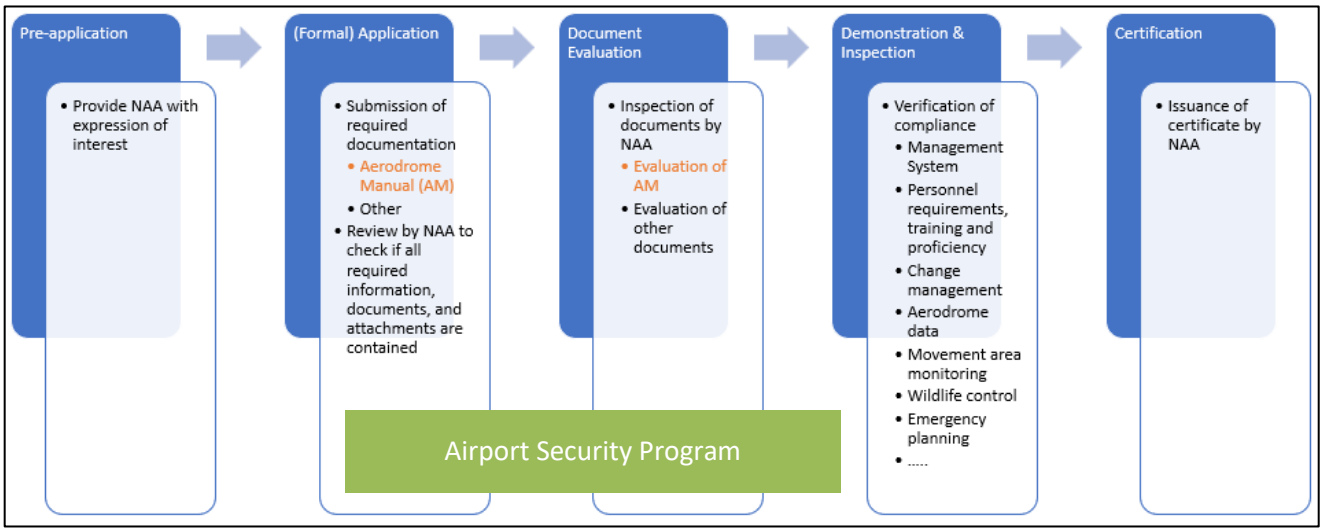


Figure 1 – Generic aerodrome certification process

[2] As described in the task 3.2.1 report "Assessment report on the existing safety and security certification requirements".

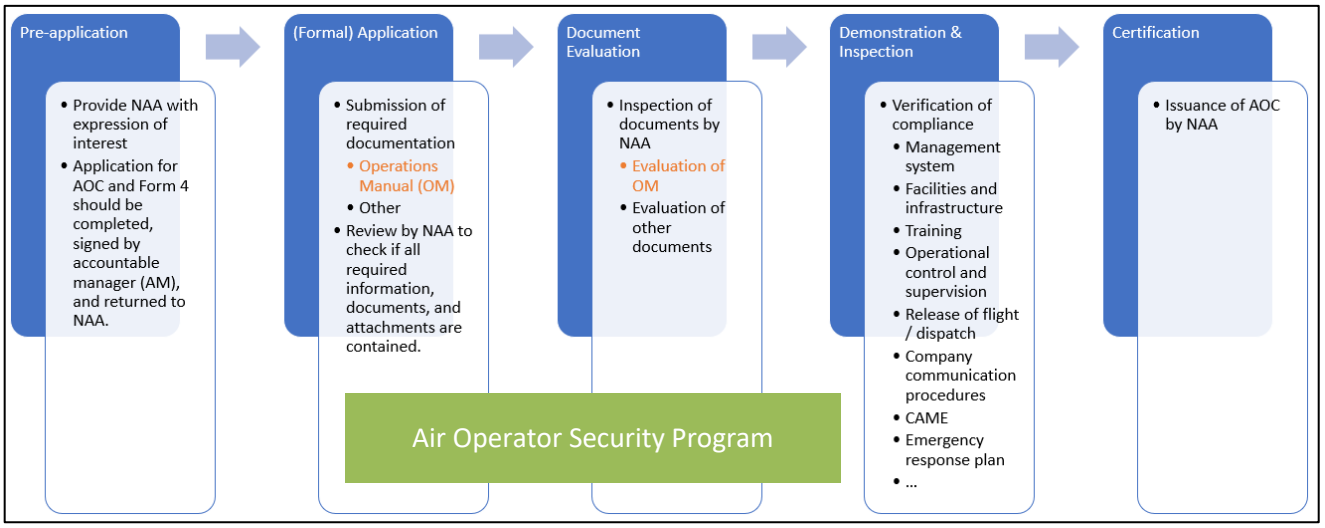


Figure 2 – Generic air operator certification process

The **Airport Security Program (ASP)** or the **Air Operator Security Program (AOSP)** are indicated as elements existing in parallel as they originate from the *Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002* (referred to later as Regulation 300/2008) which is not directly applicable for the certification process described in:

- *Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council* (referred to later as Regulation 139/2014)
- *Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council* (referred to later as Regulation 965/2012).

In this report research looked into the verification of security requirements in CAs certification practices for: **Security requirements that are directly included in regulations applicable to aerodromes or air operators' certification.**

With regards to above, the analysis conducted in D-3.2.1 indicated several security elements included in certification requirements of aerodromes and air operators (see Table 2).

Table 2: Security elements included in the certification framework of aerodromes and air operators (from the report D-3.2.1).

Security component	Aerodrome certification	Air operator certification
Least-Risk Bomb Location		X *)
Reinforced Cockpit doors		X *)
Features of aircraft design		X *)
Protection of aircraft systems		X *)
Access to the flight crew compartment		X
Aircraft security search		X
Special categories of passengers		X
Carriage of weapon		X
Alerting ATC to emergencies		X
Training of Flight and Cabin Crew		X
Procedures to handle disruptive passenger behaviour		X
Boundaries	X	
Access control and security surveillance	X	
Fence	X	
Isolated parking position	X	
Training and vetting requirements	X	X
Emergency procedures and planning	X	X
Information and data security management system	X	X

**) these elements are part of airworthiness, and as such subject to Type Certificate of an aircraft. Consequently, they are out of scope of the analysis in this report.*

Analysis in this report will provide a deepened insight into how these are assessed during the certification processes conducted at the national level in EU/EEA States.

Security requirements that are included in the aviation security regulations applicable to aerodrome (airport) operators or air operators but not directly part of the certification requirements are not in scope of this analysis.

In this context D-3.2.1 acknowledged differences between aerodromes and airport terms.[3] The analysis conducted for the purpose of this report evidenced that the regulatory coverage varies between the applicability of Regulation 139/2014 and common basic standards of Regulation 300/2008.

As a consequence, different scenarios are possible:

- States where all aerodromes being subject to EASA based certification are equally in scope of Regulation 300/2008
- States where aerodromes are subject to certification or traffic related exemption but all equally in scope of Regulation 300/2008
- States where aerodromes are subject to certification or traffic related exemption but some of them in scope of Regulation 300/2008 and some out of scope
- States where some aerodromes are not subject to certification or traffic related exemption but still in scope of Regulation 300/2008

This is illustrated in Figure 3 containing data about the number of aerodromes and airports in the EU/EEA area.

[3] See Section 4 “Terminology considerations” of the D-3.2.1 Assessment report on existing safety and security certification requirements.

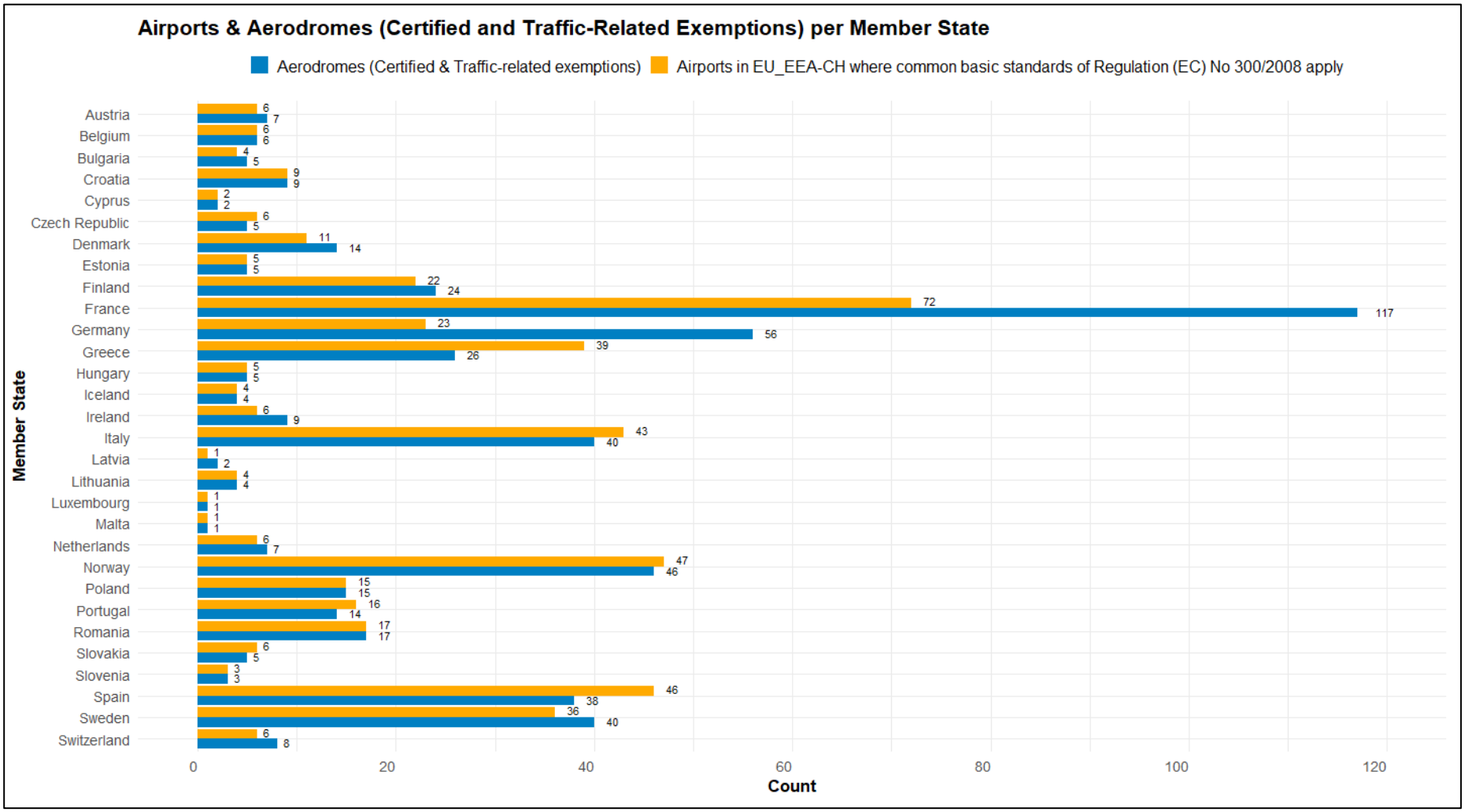


Figure 3 – Illustration of number of aerodromes and airports in the EU/EEA area

Also, in case of air operators there is no evident and clear relation between the air operator certificate (AOC) process and the applicability of security requirements unless they are directly established in the certification framework (Regulation 965/2012), for example CAT.GEN.MPA 155 and 160.

Based on the definition of "air carrier" in the Regulation 300/2008 common aviation security standards are applicable to air operators that hold the license or equivalent. This would indicate the applicability of aviation security common standards to AOC holders performing CAT operations however with no direct implications to the certification process *per se*, as the Regulation 300/2008 and its implementing acts are not included in the air operator certification framework other than for example AMC1 ORO.AOC.100(a).[4]

Mindful of the above this report is focused on investigating certification regulatory framework and practices at the national level of EU/EEA States. In the course of task D-3.2.2 the research attempted to consult stakeholders to verify the approach towards the assessment of security-related requirements listed in Table 2 in the course of aerodromes and air operators' certification. Research, at that stage, also aimed at exploring if following components are included as part of certification processes:

- Head of Security/Security manager
- Background checks
- Security policy
- Security risk assessment
- Security precautions for ground handling instructions for aircraft, passengers and cargo handling
- Security occurrences reporting
- Security training
- Security Management System

3. Methodology

This chapter outlines the process of work conducted for the creation of this report.

The objective of this deliverable D-3.2.2 was to analyse how security-related requirements are verified during the certification and if gaps or best practices can be identified.

Figure 4 shows the working process in order to achieve this task.

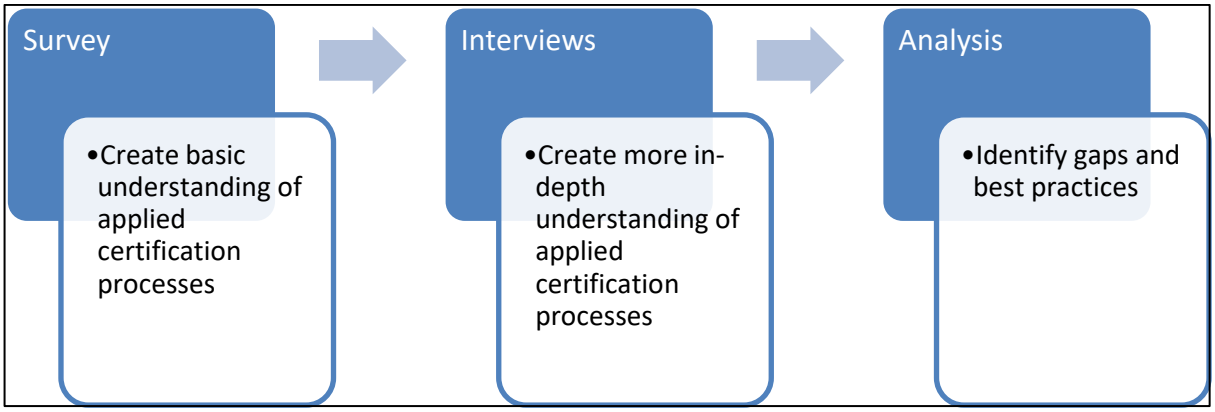


Figure 4 – Process of work

[4] EASA Easy Access rules for Air Operations and requirements applicable to commercial air transport (CAT) of passenger, cargo or mail including scheduled and non-scheduled flights, as described in Annex IV (Part-CAT).

At the initial stage the **survey** with different EU CAs, AAs, aerodrome / airport operators and air operators was conducted in order to create a basic understanding of their certification approaches (see Section 3.1 for more details). Participants were able to leave their contact details at the end of the survey if they decided they would be available to share more insight on the topic. Based on this feedback, **interviews** were scheduled and conducted. Interviews were tailored to more specific topics as a follow-up to the survey for those who agreed to it (see Section 3.2 for more details).

This allowed researchers to gather additional information on how the certification of aerodromes/airports and air operators is conducted in different EU countries and where security fits in this process. The results are listed in Chapter 4.

The combined results of the survey and interview allowed researchers to identify areas for improvement (gaps) and best practices which are discussed in Chapter 5.

Chapter 6 concludes the report.

3.1. Survey

The findings from the document analysis in D-3.1.1 were used as a baseline to draw up an online survey. The survey was intended on the one hand to validate the findings from the document analysis and on the other hand to expand on them in a targeted manner.

The survey was conducted between June and October 2024. Table 3 shows the survey questions for both the aerodromes/airports and air operators. It was divided into the topics of identification of the entity, initial contact for certification, security program (ASP/AOSP) submission, certification phases, and general comments. Some questions required users' text entries while others were multiple choice questions. Results of the survey are presented in Chapter 4.1.

Table 3: Survey structure

	Topic	Questions for aerodromes	Questions for air operators	Participant answers
	Identification			
1	**ICAO / IATA Code**	If you are the Aerodrome/Airport Operator Please enter the ICAO/IATA code	If you are the Air Operator please enter ICAO/IATA code	Text entry
2	**Authority**	If you are the Authority please enter the name of the State you refer to in your answers below	If you are the Authority please enter the name of State you refer to in your answers below	Text entry
	Initial contact			
3	**First Point of Contact for Certification**	When the applicant for aerodrome certification makes the initial contact, it needs to approach:	When the applicant for AOC makes the initial contact (at the pre-application phase) it needs to approach:	Multiple Choice
4	**National Aviation Authority (NAA)**	Please provide the full name of the National Aviation Authority (NAA) that needs to be contacted for aerodrome certification applications.	Please provide the full name of the National Aviation Authority (NAA) that needs to be contacted for AOC applications.	Text entry
	Security program submission			

	Topic	Questions for aerodromes	Questions for air operators	Participant answers
5	**Security Program**	Does the applicant for the aerodrome certification need to submit the Airport Security Program (ASP) together with the Aerodrome Manual (AM)?	Does the applicant for the AOC needs to submit the Air Operator Security Program (AOSP) together with other mandatory documents (OM, CAME, SMS, CM Manual)?	Multiple Choice
6	**ASP Submission**	If you answered "Yes" to question 5 select one of below. The ASP needs to be submitted to:	If you answered "Yes" to question 5 select one of below. The AOSP needs to be submitted to:	Multiple Choice
7	**Alternate Authority for Security**	If you answered "No" to question 5 can you briefly describe if the certification process considers ASP and at which stage?	If you answered "No" to question 5 can you briefly describe if the certification process considers AOSP and at which stage?	Text entry
8	**Security authority**	If you answered "Different authority responsible for security" in question 6, please provide the full name of it.	If you answered "Different authority responsible for security" in question 6, please provide the full name of it.	Text entry
	Certification phases			
9	**Document Evaluation Phase**	During the documents' evaluation phase, which of these occurs:	During the documents' evaluation phase, which of these occurs:	Multiple Choice
10	**On-Site Inspection Phase**	During the on-site audit/inspection/verification phase, which of these occurs:	During the demonstration and audit/inspection phase, which of these occurs:	Multiple Choice
11	**Audit Outcome**	As on outcome of the audit/inspection/verification phase, which of these occurs:	As on outcome of the demonstration and audit/inspection phase, which of these occurs:	Multiple Choice
12	**Post-Certification Oversight**	After the certificate is issued, as part of ongoing oversight, which of these occurs:	After the AOC is issued, as part of ongoing oversight, which of these occurs:	Multiple Choice
13	**Post-Issuance Phase**	After the certificate is issued, which of these occurs:	After the AOC is issued, which of these occurs:	Multiple Choice
	Comments			
14	**Further comments / suggestions**	Please add any further comments specific to the air operator certification process which might be relevant to this project, including suggestions you would like to make or issues you would like to raise.	Please add any further comments specific to the air operator certification process which might be relevant to this project, including suggestions you would like to make or issues you would like to raise.	Text entry

3.2. Interviews

Semi-structured interviews were the method used for the second stage of consultations. This is a qualitative research method that balances the adaptability of unstructured interviews with the consistency of structured interviews (Adams, 2015). While these kinds of interviews rely on a prepared set of open-ended questions, they also provide the interviewer with the flexibility to delve deeper into responses and pursue new topics that emerge during the conversation. Key features of semi-structured interviews therefore are:

- **Flexibility:** Adapt to interviewee's responses

- **Focused inquiry:** Retains structure to make sure that essential questions are covered across all interviews

The research team used a range of channels to contact stakeholders. In total 8 aerodrome (airport) operators, 4 air operators, and 8 authorities agreed to participate in the interview. As almost all of the NAAs interviewed provided experts in both, the area of aerodrome and air operator certification the research team was able to collect 15 inputs regarding aerodrome certification (8 operators and 7 authorities) and 10 inputs regarding air operator certification (5 air operators and 5 authorities).

Interviews were conducted virtually between October and November 2024 and lasted about 60 minutes each. Interviews started with an introduction of participants and the project including the aim to verify the data previously collected in the survey, and to clarify open aspects and questions. One person at CASRA led the interview while another research person took notes of the interviewee(s) answers in the interview guide (see Section 3.2.1). Notes were then sent back to each participant for amendments and endorsement. Answers were next anonymised, and aggregated to allow analysis and comparison. Results are presented in Chapter 4.2.

3.2.1. Interview guide

Part 1 of the semi-structured interview covered general questions on certification:

- **Security consideration in certification:** How much do you think is security considered in the certification process of an aerodrome/air operator in your state/country (a lot, somehow, little)? Can you provide a detailed explanation of your answer?
- **Desired security requirements in certification:** Are there any security related requirements you would particularly want to see incorporated in the certification process?
- **Preferred certification audit approach:** Which approach would you prefer in the certification process: if audits in safety and security are conducted as two separate processes or as one? Can you provide an explanation to your answer?
- **Challenges in managing safety and security:** Is there anything in the certification process of an aerodrome/air operator in your state/country that you find especially challenging/difficult to manage between safety and security?
- **Personnel familiarity with safety and security:** Are personnel from the safety domain familiar with security requirements and the other way around (a lot, somehow, little)? Can you provide detailed explanation of your answer?

Part 2 covered security elements in certification requirements that were identified in D-3.2.1:

- **Are any of these included in part of verification (analysis of manuals and/or audit) during certification?**
    - Aerodrome and Air Operator Personnel and Training
        - Security training / training programs in security
        - Security vetting (background checks)
        - Competency assessment of head of security
    - Airport Security Systems and Infrastructure
        - Aerodrome boundaries, fence, CCTV system or patrolling of access to the area inside the fence
        - Airport Identification Card System and Process
        - Lighting of the apron
        - Isolated parking position
        - Procedures for accessing the aerodrome movement area, coordination with security agencies; prevention of unauthorized entry into the movement area
    - Aerodrome and Air Operator Incident Reporting, Risk and Change Management

        - Security reporting
        - Security risk assessment
        - Impact assessment of security measures on safety
        - Security instructions, procedures, training, responsibilities and guidance considering Regulation (EC) No 300/2008.
    - Aerodrome and Air Operator Information Security
        - Information and Data Security Management
        - Identification of Critical Systems and Data
    - Aerodrome and Air Operator Security Management
        - Security policy
        - Security Management System (SeMS)
    - Aerodrome and Air Operator Emergency Preparedness
        - Emergency Procedures and Planning
        - Testing for aerodrome facilities and equipment to be used in emergencies
        - Exercises to test Emergency Plans
        - Air Operator Security Program
        - Alerting ATC of Emergencies
    - Air Operator Procedures
        - Carriage of weapons
        - Procedures of handling disruptive passengers (on board and on the ground)
        - Special categories of passengers
        - Aircraft protection
        - Aircraft search
        - Security precautions for ground handling instructions for aircraft, passengers and cargo handling
        - Use of restrain devices
        - Admission to flight crew compartment (including persons other than the flight crew)
        - Access to flight deck

Part 3 of the interview covered challenges, gaps, and best practices in aerodrome and aircraft operator certification:

- **Safety and security process alignment:** Would you prefer security and safety processes for verification of conformity being more synchronised or separated? Can you provide an explanation to your answer?
- **Gaps in safety-security certification:** What are the main gaps you could identify in current certification of aerodromes and aircraft operators in the context of safety and security?
- **Best practices for safety-security coordination:** What are the best practices you could recommend to ensure coordination of safety and security requirements in the context of certification?

4. Results

This chapter shows the results for:
- the survey (Section 4.1)
- the follow-up interviews (Section 4.2)

4.1. Survey

Figure 5 shows the coverage of European countries participating in the survey (34 replies concerning aerodromes and 35 concerning air operators).

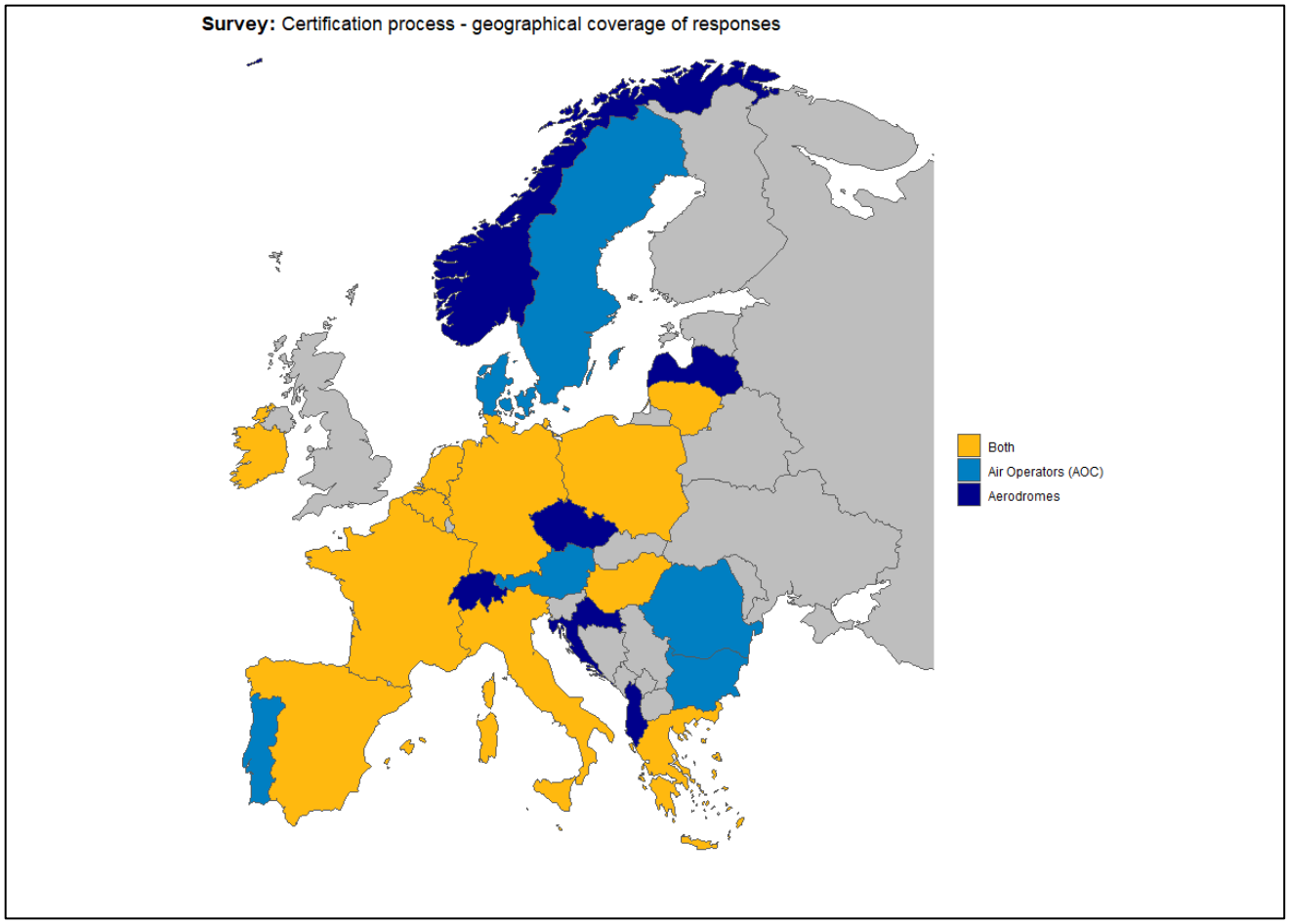
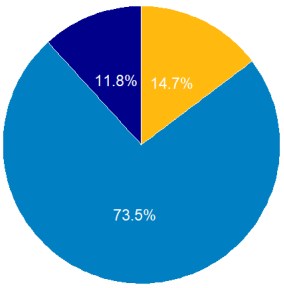
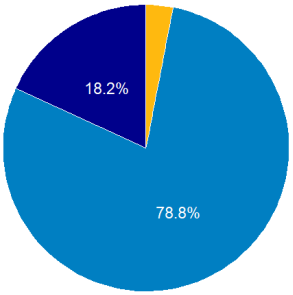


*Figure 5 – Coverage of European countries participating in the survey (*Both indicates that at least one reply in the scope of aerodrome and air operator within a country was received through the survey)*

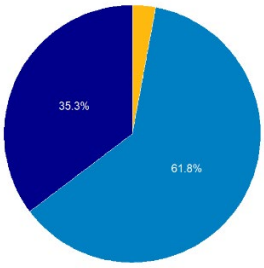
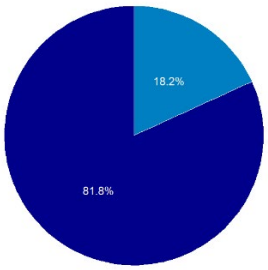
The following graphs show the survey results for the multiple-choice questions with regards to aerodromes (left side) and air operators (right side) in the scope most relevant for the purpose of this report.

4.1.1. Initial contact

When the applicant for aerodrome / air operator certification makes the initial contact, it needs to approach:

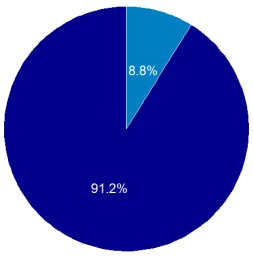
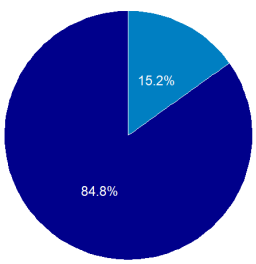
Aerodrome	Air operator
both separately, National Aviation Authority (responsible for safety) and the Appropriate Authority (responsible for security) only National Aviation Authority which is responsible for both, safety and security only National Aviation Authority which is responsible for safety	
	

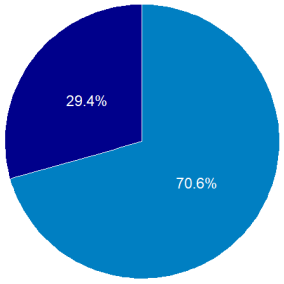
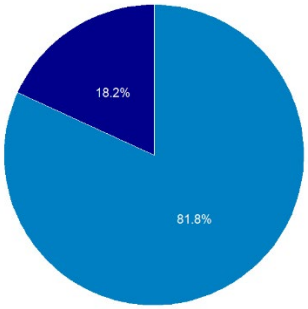
4.1.2. Security program submission

Aerodrome	Air operator
Does the applicant need to submit the ASP together with the AM?	Does the applicant need to submit the AOSP together with other mandatory documents?
Yes No I do not know	
	

4.1.3. Document evaluation phase

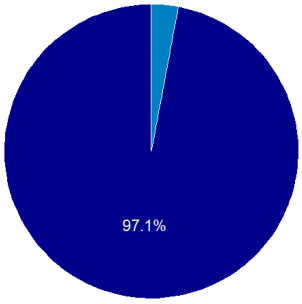
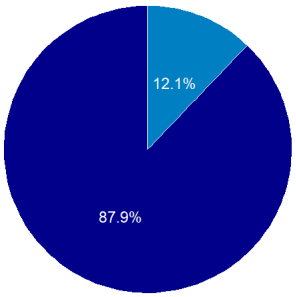
During the document's evaluation phase, which of these occurs:

Aerodrome	Air operator
ASP is assessed separately from the Aerodrome Manual Assessment of all Manuals is coordinated	AOSP is assessed separately from other Manuals Assessment of all Manuals is coordinated
	

Aerodrome	Air operator
References in ASP to Aerodrome Manual (or other Manuals) are not permitted References in ASP to Aerodrome Manual (or other Manuals) are permitted	References in AOSP to other Manuals are not permitted References in AOSP to other Manuals are permitted (e.g. OM A, OM D, SMS, CM)
	

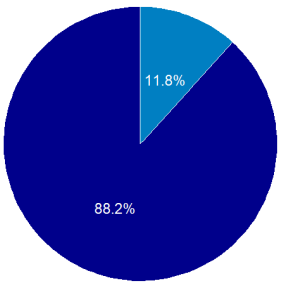
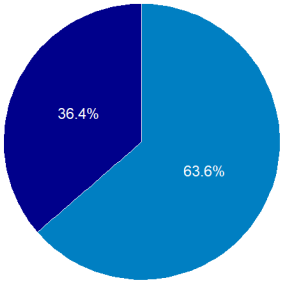
4.1.4. On-site inspection phase

During the on-site audit/inspection/verification phase, which of these occurs:

Aerodrome	Air operator
Audit/inspection/verification in safety and security are conducted as two separate processes Audit/inspection/verification is coordinated between safety and security	
	

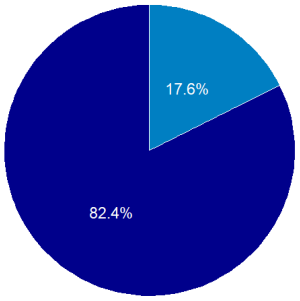
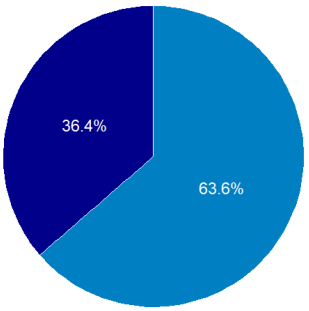
4.1.5. Audit Outcome

As an outcome of the audit/inspection/verification phase, which of these occurs:

Aerodrome	Air operator
Non-conformities in security do not stop the certification issuance process Non-conformities in security need to be fully rectified otherwise certification process will stop	Non-conformities in security do not stop the AOC issuance process Non-conformities in security need to be fully rectified otherwise AOC process will stop
	

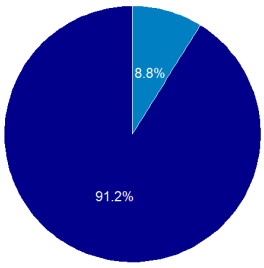
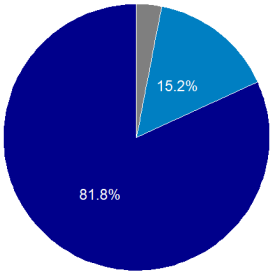
4.1.6. Post-certification oversight

After the certificate is issued, as part of ongoing oversight, which of these occurs:

Aerodrome	Air operator
Non-conformities in security do not impact the certification Non-conformities in security may result in the certificate being suspended	Non-conformities in security do not impact AOC Non-conformities in security may result in AOC being suspended
	

4.1.7. Post-issuance phase

After the certificate is issued, which of these occurs:

Aerodrome	Air operator
Full re-certification occurs only in certain circumstances There is mandatory recurrent full re-certification NA	
	

4.2. Interviews

Figure 6 shows the coverage of EU/EEA countries participating in the follow-up interviews. In total, a number of 20 interviews[5] were conducted where 5 of them covered both certification of aerodromes and air operators. The other 10 interviews covered aerodrome certification and the remaining 5 air operator certification specifically.

[5] One stakeholder was not interviewed but rather sent the questionnaire in a written format. Due to lack of possibility for the follow-up and to clarify several items this input was taken into account in the limited scope only.

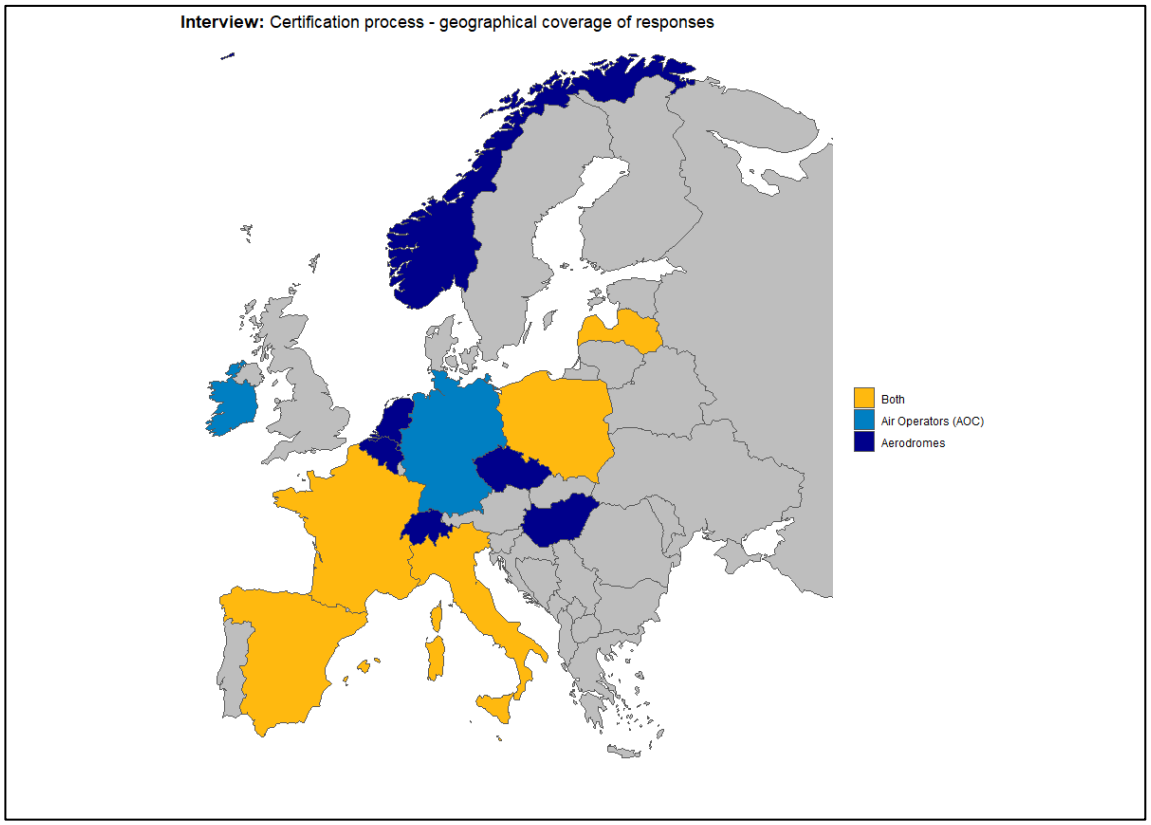


Figure 6 – Coverage of European countries participating in the interviews

Figure 7 shows that over 30 experts were interviewed altogether (as some organisations provided a broader representation) and the overall number of interviewees per the domain of expertise – safety, security or both.

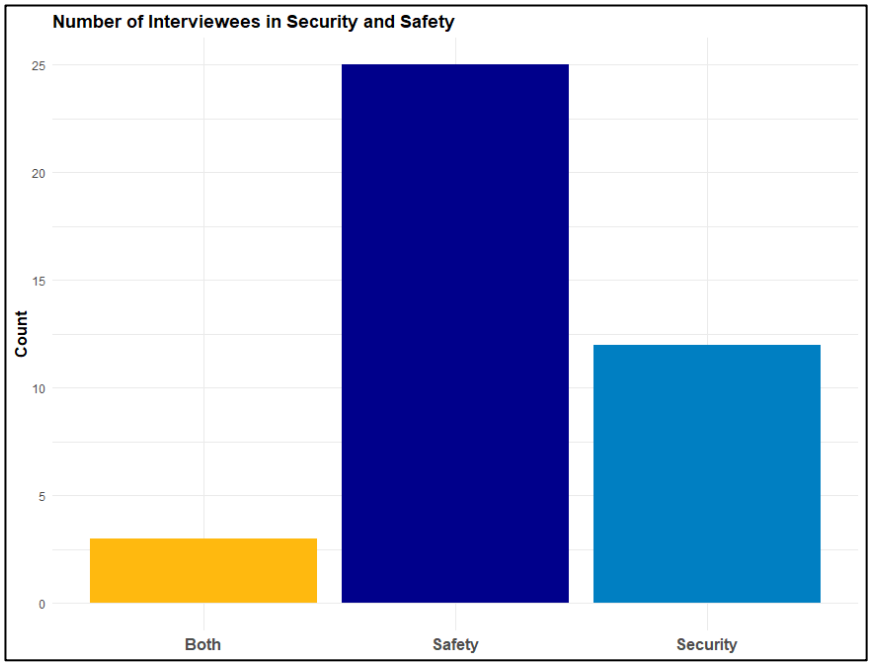


Figure 7 – Number of interviewees in either security only, safety only, or both (security & safety)

The following sections present the interview analysis per topic (see again Section 3.2.1 "Interview guide"). Aggregated answers to Part 1 and 3 of the interview are in the Appendix.

4.2.1. Security consideration in certification

From the perspective of arrangements at the authority level, interviews' feedback was aligned with early indications of the survey. The survey replies showed that in case of an overwhelming majority both, the Airport Security Program (ASP) and the Air Operator Security Program (AOSP) are assessed separately, even if they are submitted to the same authority (responsible for both, safety and security). There has also been a noticeable difference identified between the ASP and AOSP with the former in the majority of cases not required to be submitted together with the Aerodrome Manual (AM).[6]

In terms of arrangements at the authority level, input from interviews showed that there are **two main organisational models**:

- One authority responsible for safety and security regulatory oversight being the Competent Authority (CA) for safety and at the same time the Appropriate Authority (AA) for security.
- Two separate authorities, where one is responsible for safety and another is responsible for security.

These two models were indicated in 98% of responses related to air operators and 85% or responses related to aerodromes certification with the first model being more common among interviewed EU Members.

Interviews provided additional insight about detailed arrangements applicable to the first model. In this solution there is typically a clear competence assignment resulting in different departments (organisational units) responsible for:

- Aerodromes certification
- Air Operators certification
- Security conformity (in some instances actually upgraded to the security certification as established by the national framework)

All these elements have been indicative of a structural separation which could potentially result in substantial segregation and a lack of connection between certification and verification of security requirements. Also, most of the responses were indicative of very insignificant connection between security and aerodromes' and air operators' certification. Observations based on answers to this interview question include the following:

- Consideration to security requirements in certification is limited.
- Coordination with security assessment process is focused on requirements included and specified for aerodromes or air operators and originating directly from certification regulatory framework (for example CAT.GEN.MPA 155 and 160 for air operators or CS ADR-DSN.F.370 for aerodromes)
- Security related requirements are typically either verified by the organisational unit responsible for security based on ASP or AOSP assessment or looked at by both safety and security. Security organisational units at the authority level are most often assigned with several security tasks including oversight of other entities e.g. regulated agents, in-flight supplies' suppliers etc.
- Requirements related to aviation security regulations which are not in the direct scope of certification framework are not formally included in the certification process and would not have direct impact on overall conformity assessment in this process.

[6] This is due to the differences in the scope of certification which covers the aerodrome and the security scope that refers to an airport. Report D-3.2.1 defined airport as the *certified aerodrome from/to where commercial operations are conducted and which is equipped with facilities enabling processing of passengers, baggage and cargo for purposes of commercial transport.* The aerodrome certification does not include facilities used for passengers, baggage and cargo (and related processes).

- Indirect connection between certification and verification of security requirements is established on the basis of approval, acceptance or endorsement of the ASP or AOSP, if one is required for the certification process completion. Such an approach was noted, it is however not uniformly implemented as some aerodromes for example complete their certification first and the approval of security measures applicable to the airport follows on the basis of ASP and security audit.
- In few individual cases there is a separate certification process related to airports and air operators specifically established by the national framework. This process is parallel to the safety certification.

4.2.2. Desired security requirements in certification

In most cases, there were no specific suggestions with regards to expanding to new specific security requirements in the certification process, stakeholders rather acknowledged the value of stable current processes. This was even more evident in instances where separate security certifications of airports and air operators has been established. This could be related to structural and formal arrangements with the separate regulatory frameworks and separation at the authority level influencing the perspective of stakeholders in relation to this question.

Generally, stakeholders did not favour including additional operational security assessments in the certification process of aerodromes and air operators, especially if such an assessment would need to be performed by safety domain representatives. The main reason indicated was the need for an extensive subject-matter expertise which is not easily available in the safety domain.

Typically, stakeholders recognized the existence of areas that currently relate to both, safety and security, in aerodromes and air operators' certification. These areas were aligned with the identified ones in the report D.3.2.1 and were confirmed by interviewees. In this context the following elements were mentioned if the interviewee(s) subjectively felt they are not considered enough during the certification:

- perimeter fence
- aerodrome boundaries
- lighting of apron
- emergency, contingency and response procedures

It is worth noting that suggestions were made regarding the consistency of the security management approach. Since SMS (Safety Management System) and ISMS (Information Security Management System) are already mandated for implementation by aerodromes (airports) and air operators, elements of SeMS (Security Management System) were discussed. However, these were presented more as best practices rather than concrete proposals to amend the certification process. These stakeholders seem to be interested in a more integrated approach especially with regards to the evaluation of organisational arrangements (management of safety and security) during the certification. Among these elements mentioned were:

- Integrated (or interconnected / interacting) risk management,
- Change Management process and its applicability to changes triggered by security
- Reporting
- Accountability concept

4.2.3. Preferred certification audit approach

Consequently, and having in mind previously mentioned factors (organisational arrangements at the authority level, separate submissions of ASPs and AOSPs) the dominant approach expressed in interviews was in favour of separate processes for safety and security conformity evaluation in the certification process.

This approach was based on:

- Differences in scope and concepts between safety and security
- Need to ensure in-depth assessment of either domain by subject-matter experts
- Requirement of detailed safety and security competence which seemed neither practical nor realistic to be combined among the same personnel
- Confidential nature of security provisions and requirements limiting access to requirements for the safety domain
- Differences in assessment methodology

Nevertheless, some stakeholders interviewed recognized potential benefits of considerations related to a more integrated approach which could include:

- Enhanced understanding of respective domains
- Potential efficiencies in resolution of findings
- Leveraging similarities in processes that apply to both, safety and security (management, training, reporting)
- Alignment of assessment methodologies
- Improved identification of areas where safety and security may impact each other

4.2.4. Challenges in managing safety and security

In the majority of cases no specific challenges were identified by stakeholders. Several stakeholders however indicated that:

- The amount of regulations jointly for safety and security is overwhelming
- Overlapping areas between safety and security pose a challenge in itself and lack clearer guidance on safety-security relationships
- Information security (related to Part-IS) component will require substantial additional effort and coordination between domains as well as inclusion of additional experts due to the nature of the subject
- Change management process is not equally applicable in security domain as it is in safety resulting in potential systemic gaps in management in general
- Specifically for air operators' certification, the challenge related to the management system and documentation review stage (interdependence of OM and AOSP documents)
- Specifically for air operators - group operations[7] approval and oversight and differences between AOC requirements as well as AOSP national requirements

4.2.5. Personnel familiarity with safety and security

Interviews evidenced varying degrees of familiarisation of safety personnel with security requirements and vice-versa. This was investigated mostly in reference to personnel conducting conformity assessments during

[7] https://www.easa.europa.eu/en/document-library/general-publications/guidance-oversight-group-operations

the certification or representing entities during the certification and did not generally refer to front-line personnel.

In this context stakeholders typically indicated that for practical reasons it would be very difficult to ensure that persons conducting the assessment within the safety certification are equally competent in the security domain and vice-versa. Authorities are more likely to provide for separate domain specific expertise and coordination between experts to ensure overlapping areas are evaluated from both perspectives (e.g. fence).

4.2.6. Safety and security process alignment

Separation of assessment between safety and security requirements is a dominant approach and broadly endorsed by the interviewed authorities' representatives, however many stakeholders encouraged coordination or synchronisation provided it brings tangible benefits and advantages. As such several items were raised:

- Enhanced information sharing
- Coordination mechanisms when needed (in terms of specific items subject to evaluation or at the evaluation methodology level)
- Analysis of potential efficiencies if integration would apply to specific elements (e.g. risk management, security reporting, SMS/SeMS)

5. Discussion

This chapter investigates details of verification of security elements during certification of aerodromes and air operators:
- Aerodromes (Section 5.1)
- Air operators (Section 5.2)
- Gaps (Section 5.3)
- Best practices (Section 5.4)

Since certification is a regulatory process, the research initially focused on understanding the distribution of competences at the national level.

Each of the EASA Member States (EU and associated States) designated the Competent Authority.[8] These authorities are in the vast majority of cases, also the Appropriate Authority for aviation security. Among EU States interviewed also a different model was identified where security matters are dealt with by another State organisation. In these cases, aviation security matters are typically handled by the governmental body related to home affairs.

At the same time, even in instances where safety and security are parts of the same authority (CA/AA) they are usually separated internally into different units. Departments or equivalent organisational units responsible for aviation security usually operate in coordination but independently from these responsible for certification and/or safety oversight of aerodromes and air operators.

In this context, there has been no specific connection identified between the depth or scope into which security is considered in the certification of aerodromes and air operators and the organisational arrangements at the authority level.

This means having the safety and security with the same Authority did not result in security being considered particularly more in the certification process. Based on answers during interviews, arrangements are typically in place to develop and maintain coordination, information exchange schemes and alignment of overall objectives and vision. These coordination arrangements are typically present, regardless if they occur within one or between two Authorities, however achieving alignment within one single Authority appears to be relatively easier.

5.1. Aerodromes certification

CAs have process(es) in place to initiate the aerodrome certification (see Table 4). This process includes the liaison with the applicant. This is organised usually in the format of the meeting and information exchange where applicable rules are explained also in terms of processes related to safety and security requirements.

[8] https://www.easa.europa.eu/en/domains/international-cooperation/easa-by-country

Table 4: Security evaluation during aerodromes' certification

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
Boundaries	Assessment of security related component is not required per certification rules	Applicant is informed about requirements related to establishments of aerodrome boundaries including about approvals or permits needed from the security perspective (GM1 ADR.AR.C.015)	It is the applicant responsibility to comprehend dependencies between aerodrome certification requirements for aerodrome boundaries and specifications related to security zones of an airport. GM1 ADR.OR.B.015 (b)(2) states "*aerodrome boundary should not be confused with the boundaries established for other purposes, such as fences, the land ownership boundaries used by local planning authorities, or those used to designate security restricted zones.*"	Typically assessed by the Security responsible authority as a part of the ASP evaluation.
Access control and security surveillance	Assessment of security related component is not required per certification rules	NAAs verifies process to ensure vehicle drivers have necessary authorisation and are trained on the rules of using vehicles when present in the movement areas. Rules of marking and lighting of vehicles are also included (ADR.OPS.B.024 and ADR.OPS.B.080) Control of movement of passengers and personnel is also subject to assessment (ADR.OPS.B.033). Apron floodlights (ADR.DSN.M.750	There is only a very general indication of the need to coordinate with security authorities in relation to control of passengers' movement in the movement area and other operational areas of aerodrome (meaning excluding the terminal) (AMC1 ADR.OPS.B.033 (a). There is no link established with any process related to background checks, access control, CCTV, patrols or airport identification card system.	Typically assessed by the Security responsible authority as a part of the ASP evaluation.
Fence	Assessment of security related component is required per certification rules.	CAs have process to verify protective role of fencing to prevent access to aerodrome (CS- ADR-DSN.T.920) as well as in relation to emergency access and service roads CS ADR-DSN.T.900)	There is clear link with security when describing the safety objective of fencing in using the terms unauthorised person. The wording of CS ADR-DSN.T.920 may be ambiguous between points (c) (2) and (d) however the overarching purpose is to deter and prevent access where this could be of a safety risk. Another interesting component relates to the fact that certification accounts for fencing only and does not consider other methods of unauthorized access prevention and detection. It is only in GM1 ADR-DSN.T.920 where "the fence or barrier" is mentioned. This resulted in inconsistency in replies to interview questions as the relevant point covered other elements (e.g. CCTV)	Typically assessed by both the Security and Safety responsible authority with different perspectives.

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
Isolated parking position	Assessment of security related component is required per certification rules.	CAs have process to verify the establishment of isolated parking position and its role in the emergency planning (CS ADR-DSN.F.370) as well as in relation to emergency planning (GM3 ADR.OPS.B.005 (a))	There is no specific security regulation beyond CS ADR-DSN.F.370	Typically assessed by both the Security and Safety responsible authority with different perspectives.
Training and vetting requirements	Assessment of security related component is not required per certification rules	In terms of the authority representatives every CA ensures necessary qualifications of its personnel conducting certification. The communication with security experts is ensured as well (ADR.AR.005.B) In terms of aerodrome organization - certification covers assessment of the accountable manager and verification of training and competency assessments of personnel (ADR.OR.D.015 and ADR.OR.D.017)	Neither the accountable manager nor personnel training and proficiency checks include specific notion in relation to security requirements and no reference to aviation security common standards (Regulation 300/2008).	Typically assessed by the Security responsible authority as a part of the ASP evaluation. Safety only checks for general existence of training programs.
Emergency procedures and planning	Assessment of security related component is required per certification rules	CAs ensure assessment of emergency procedures and planning (ADR.OPS.B.005)	Evident link due to the fact that some emergencies may be related to security events.	Typically assessed by both the Security and Safety responsible authority with different perspectives.
Information and data security management system	Assessment of security related component is required per certification rules	CAs assess the security for the aeronautical data processing	The link is established through the requirement to implement information security management system in relation to aeronautical data.	Typically assessed by Safety responsible authority. Enlargement in terms of scope expected in relation to Part-IS implementation

As mentioned in the previous section, the applicability scope of aerodrome certification is not the same as the applicability of the aviation security framework based on Regulation 300/2008. Aerodrome certification covers as per the "aerodrome" definition areas (including buildings, installations or equipment) used wholly or in part **for the arrival, departure and surface movement of aircraft**. This will typically not include terminal buildings or cargo warehouses. In the scope of the airport, the aviation security framework covers areas defined as landside, airside, security restricted area (and critical part thereof), demarcated area and processes related to these delineations. Table 5 illustrates definitions in the respective regulations.

Table 5: Security and safety definitions for aerodrome / airport

Safety definitions (139/2014, 2018/1139)
Movement area - part of an aerodrome to be used for the take-off, landing and taxiing of aircraft consisting of the manoeuvring area and the apron(s)
Manoeuvring area - part of an aerodrome to be used for the take-off, landing and taxiing of aircraft, excluding aprons
Apron - means a defined area intended to accommodate aircraft for purposes of loading or unloading passengers, mail or cargo, fuelling, parking or maintenance;
Aircraft stand – means designated areas on an apron intended to be used for parking an aircraft

Security definition (300/2008, 272/2009 1998/2015)
Airside – **movement area of an airport**, adjacent terrain and buildings or portions thereof, access to which is restricted
Security restricted area – an area of airside where, in addition to access being restricted, other aviation security standards are applied;
Critical part of the security restricted area – shall include at least the following: (a) all parts of an airport to which screened departing passengers have access; and (b) all parts of an airport through which screened departing hold baggage may pass or in which it may be held, unless it concerns secured baggage. A part of an airport shall be regarded as a critical part at least for the period of time that the activities referred to in points (a) or (b) are taking place. The definition of critical parts of security restricted areas shall ensure that there is no contamination of screened departing passengers (both originating and transfer) and their cabin baggage as well as of screened departing hold baggage (both originating and transfer).
Demarcated area - an area that is separated by means of access control either from security restricted areas, or, if the demarcated area itself is a security restricted area, from other security restricted areas of an airport
Landside - those parts of an airport, adjacent terrain and buildings or portions thereof that are not airside

Airside is not defined in the safety EU Regulation but referred to in Guidance - GM1 ADR.OPS.B.024(a). This guidance mentions that airside may encompass other areas than the movement areas, in which vehicles may be operating for various purposes. Examples, of parts which are not movement area, would be service roads between the terminal buildings and aprons, perimeter roads, parking spaces of vehicles and ground support equipment.

In the security context airside encompasses runways, taxiways (manoeuvring area) and aircraft stands (apron) through inclusion of the term “movement area” causing this to be the overlapping area with safety. Any further decision to include further areas into the “airside” is left to the discretion of airport (aerodrome) operators as the only condition defining an area as “airside” is, that it is covered by the access control measures (“access to which is restricted”). To increase security protections of certain parts of the airside, security restricted areas shall be established. In this case other (additional) security measures would apply. In accordance with EU Regulation 1998/2015 at least following areas shall become security restricted area:

- part of an airport to which screened departing passengers have access; and
- a part of an airport through which screened departing hold baggage may pass or in which it may be held, (unless it concerns secured baggage); and
- a part of an airport designated for the parking of aircraft to be boarded or loaded.

A further elevation of the security status is possible by establishing critical parts of security restricted areas. These shall be established and include:

- part of an airport to which screened departing passengers have access; and
- a part of an airport through which screened departing hold baggage may pass or in which it may be held, (unless it concerns secured baggage);

Additionally, demarcated areas can be established within airside in accordance with EU Regulation 1254/2009.

Adding to the complexity, boundaries between all these security zones must be clearly identifiable as different security measures apply when moving between these zones.

As illustrated by the analysis of these regulations equally applicable to the same aerodrome area – movement area – security has a much more complex model, unless the entire airside / movement area is considered a critical part of the security restricted area. Additionally, security restricted area (or critical parts thereof) may be established outside of the movement area, for example in the terminal building.

The assignment of areas to a specific security status is defined as a mix of infrastructure and the function they play in the set of protective (preventive) security measures and depending which activities are performed there (see Table 6).

All these interdependencies cause those areas indicated most often as overlapping by interviewees was in relation to access control, fences and boundaries. In the safety domain the focus is on unintentional occurrences therefore the verification of barriers and measures is rather the responsibility of the security domain with the assumption that robust security measures will ensure an adequate level of safety.

Table 6: Security zones and related infrastructure elements and security processes

Security zone of an aerodrome/airport	Infrastructure element	Security process related
Airside	Runways Taxiways	Movement of authorised persons and vehicles Activities not requiring persons to be screened
Security restricted area	Apron Service roads Parts of the terminal (e.g. jetways, baggage sorting areas – as long as they are located beyond screening) Airport busses	Boarding or loading of an aircraft Passenger and baggage screening Passenger and baggage protection
Critical part of the security restricted area	Apron Service roads Parts of the terminal (e.g. jetways, baggage sorting areas – as long as they are located beyond screening) Airport busses	Passenger and baggage screening Passenger and baggage protection
Demarcated area	Any area of the airport	Any process covered by alternative security measures applicable to specific operations[9]

[9] 1. aircraft with a maximum take-off weight of less than 15 000 kilograms;
2. helicopters;
3. state, military and law enforcement flights;
4. fire suppression flights;
5. flights for medical services, emergency or rescue services;
6. research and development flights;
7. flights for aerial work;
8. humanitarian aid flights;
9. flights operated by air carriers, aircraft manufacturers or maintenance companies, transporting neither passengers and baggage, nor cargo and mail;
10. flights with aircraft with a maximum take-off weight of less than 45 500 kilograms, owned by a company for the carriage of own staff and non-fare-paying passengers and goods as an aid to the conduct of company business;
11. flights with aircraft with a maximum take-off weight of less than 45 500 kilograms, chartered or leased in its entirety by a company from an aircraft operator with which it has a written agreement for the carriage of own staff and non-fare-paying passengers and goods as an aid to the conduct of company business;
12. flights with aircraft with a maximum take-off weight of less than 45 500 kilograms, for the carriage of the owner of the aircraft and of non-fare-paying passengers and goods.

Another aspect which was mentioned as overlapping is in relation to emergency procedures. This is the consequence of the nature of incidents and accidents as very often the procedures could be similar or cross-referenced. In this context the most frequently raised element was "isolated parking position" at an aerodrome. It is worth noting that aviation security regulatory framework does not contain detailed specifications related to security related emergency procedures.

Finally, information security management systems were identified as an area of overlap or interdependence including the upcoming evolution from current Aeronautical Data Quality only towards the comprehensive system based on Part IS.

Even with differences between the aerodrome and the airport it is important to note that aerodromes shall implement a management system (ADR.OR.D.005) which would be applicable to an aerodrome operator. It is actually the aerodrome operator that is an entity applying for the aerodrome certification. This entity will typically be the same as an airport operator (with few exemptions when the airport terminal is managed by a different organisation). In this context, both topics – safety and security – are shared by the same organisation in terms of management. The research revealed such organisations are required to implement SMS (ADR.OR.D.005) and "security management system" for aeronautical information and data (ADR.OR.D.007) but not the SeMS to manage aviation security. At the same time the Regulation 300/2008 requires airport operators to implement several processes that are reflective of SeMS processes, including at least:

- risk assessment (1.0.6 of the Annex to the Regulation 1998/2015)
- internal quality control (art 12 the Regulation 300/2008)

Additionally, the security reporting is strongly encouraged, following the Annex 17 provisions and ICAO Guidance and may potentially soon become part of the EU aviation security common basic standards.[10]

Moreover, 1.1.1 of the Annex 1 to the Regulation 300/2008 contains a limited but still valid notion of change management. Even if limited to *designing and constructing new airport facilities or altering existing airport facilities* it requires considering aviation security standards in these processes. Nevertheless, this does not constitute full integration of security into the overall change management (as designed per SMS concept) as it assumes only a one-directional relationship where some operational or infrastructural changes could impact security. It does not take into account other processes where:

- other changes (organisational, process) which can impact security
- security changes that can have impact on security
- security changes that can have impact on safety

To achieve increased security improvement and benefit from the holistic overview of security posture all these elements should be incorporated in the change management consideration involving security to the fullest extent.

The second set of elements are those related to the management system where certain process overlaps were identified. As per aerodromes' certification requirements an SMS needs to be implemented. This results in a structured approach which covers the following elements:

- Accountable Manager
- Change Management
- Nominated Persons (Postholders)
- Safety Policy
- Processes and procedures

[10] https://www.icao.int/Security/SFP/Pages/Incident-Reporting-Guidance-and-Taxonomy.aspx

- Risk Management
- Reporting

The research then explored if any of these following elements relate to managing security and elements listed in section 2.2 and if so, what are the touchpoints during the aerodrome certification:

- Head of Security/Security manager
- Background checks
- Security policy
- Security risk assessment
- Security occurrences reporting
- Security Management System

The most often mentioned element which appeared in replies was in relation to security reporting. The reporting system in general is assessed during the certification evaluation however, this is not specifically included in the evaluation to determine the extent of security coverage in it.

The remaining elements are subject to an assessment based on ASP and through the security audit and lead by representatives of the security domain. However, except for one EU State, none had SeMS introduced into their National Civil Aviation Security Program.

5.2. Air Operators certification

In terms of air operators, the foundation of certification is based on article 30 of the Basic Regulation. This provision refers to further requirements established by the virtue of article 29 and related Annexes V, VI and VII. For the purposes of the analysis in this report the most essential are provisions of Annex V – requirements for air operations as well as requirements for the Operation Manual content as indicated by AMC3 ORO.MLR.100.

Section 6.2 of the report D-3.2.1 described the general framework of the certification under EASA rules. In accordance with the article 3 of the Regulation 956/2012 each Member State shall appoint the Competent Authority (CA) responsible for the certification (of air operators).

The main assumption and focus of this report is related to the CA (also called National Aviation Authority, or NAA) carrying out this task, being mindful of derogations which are allowed in line with article 65 of the Regulation 2018/1139[11] (see Table 7).

[11] EASA AOC: to cert or not to cert, February 2021 - https://www.lexology.com/library/detail.aspx?g=bb8f7b52-d59e-4867-a9e9-dc42af128566

Table 7: Security evaluation during air operators' certification

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
Aircraft Operator Security Programme	Assessment of security related component is required per certification rules (AMC1 ORO.AOC.100(a)	Based on interviews replies, typically AOSP is submitted either together with other manuals required for AOC certification or separately	The AMC clearly indicates that in accordance with Regulation (EC) No 300/2008, as part of granting the AOC, the CAT operator should provide the competent authority with the operator's security programme, including security training. The security programme should be adapted to the type and area of operation, as well as to the aircraft operated.	The AOSP is assessed by the organisational unit responsible for security (as a part of the CA or separate governmental body). Certification responsible structure acknowledges the assessment by security domain but does not perform assessment themselves
Training Programmes Training and vetting requirements **Training of Fight and Cabin Crew**	Assessment of security related component is partially required per certification rules – this is in the scope of training *(8.4 of Annex 5 to the Reg. 2018/1139)* of air operator crew *(AMC1 ORO.GEN110(a), CC.TRA.200 of the Regulation 1178/2011)* as well as the ground personnel *(ORO.GEN.110(a), especially AMC2 ORO.GEN110(a))*	CAs have process in place to verify general training requirements. They are typically described in Part D of the OM of air operator.	AOSP would typically include security training requirements. The alignment of these provisions with OM Part D is the responsibility of the air operator. Training requirements in the AOSP are assessed by the organizational unit in charge of the oversight of the Regulation 300/2008. These training requirements are described in extensive details in the Regulation 2015/1998 (implementing act to the Regulation 300/2008). Vetting is not included in the CAT.GEN.MPA.175 or in AMC3 ORO.MLR.100 Section 5 – Qualification requirements.	Typically assessed by security responsible authority as a part of AOSP. AMC1 and AMC2 are not specific enough containing only general reference to the Regulation 300/2008. Also supporting Guidance - GM1 ORO.GEN.110(a) is inaccurate. Air operators have not enough guidance in relation to the content of the training creating a potential gap in the training for crew and personnel responsible for "passengers, baggage, cargo, mail, equipment, stores and supplies intended for carriage so that they contribute to the prevention of acts of sabotage or other forms of unlawful interference. "

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
Procedures to handle disruptive passenger behaviour **Use of restrain devices**	Assessment of security related component is required per certification rules *(8.3 of Annex 5 to the Reg. 2018/1139)* as well as *CAT.GEN.MPA.105 (a) (4) (5)*	CAs generally have process in place to verify procedures related to "unruly" passenger behaviour as these shall be reflected in OM A (AMC2 8.2.3, 8.3.11, 11 (f), this is however not consistently assessed as a part of the certification activity done by the organisational unit competent for AOC certification and requires significant coordination with security domain.	General rules are evaluated however details of procedures are also contained in the AOSP and assessed by the organisational unit in charge of the oversight of the regulation 300/2008. Regulation 300/2008 does not contain elements related to unruly behaviour	Typically assessed by both, safety and security responsible authority.
Access to flight crew compartment **Security of flight crew compartment**	Assessment of security related component is required per certification rules *(8.4 of Annex 5 to the Reg. 2018/1139)* and ORO.SEC.100 and related CAT.GEN.MPA.135	Consistently assessed by CAs during the air operator certification process by the organisational unit responsible for air operator certification and as described in OM A	Regulated by Annex 8 and aircraft design specifications as well as security provisions of aircraft operations. Also present in the security Regulation 300/2008	Typically assessed by safety responsible authority.
Carriage of weapons	Assessment of security related component is required per certification rules (CAT.GEN.MPA.155 and 160)	CAs generally have process in place to verify procedures of weapon carriage as they shall be reflected in OM A 9.2. This is however not consistently assessed as a part of the certification activity done by the organisational unit competent for AOC certification and requires coordination with security domain.	Both, safety and security regulations contain provisions related to the carriage of weapons and detail cross reference is provided	Typically assessed by both, safety and security responsible authority.

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
Aircraft security search (and check) **Aircraft search procedure checklist**	Assessment of security related component is required per certification rules *(8.4 of Annex 5 to the Reg. 2018/1139)* and in terms of training *(AMC1 ORO.GEN110(a))*	CAs generally has no clear reference to verify procedures of aircraft search. Assessment requires coordination with security domain also due to non-public character of some provisions.	Aspect regulated by both domains however no clear recognition of potentially different processes between: - aircraft search or check per Annex 17 4.3.1 - aircraft search per Annex 6, 13.13 There is only very limited reference in the AMC1.ORO.GEN.110 (a) requiring training program for the cabin crew to cover aircraft search related to 300/2008, plus general indication of Section 10 of the OM A in the AMC3 ORO.MLR.100 Regulation 300/2008 does not address the provisions of Annex 6, 13.13	Typically assessed by security responsible authority.
Special categories of passengers	Assessment of security related component (transportation of deportees, inadmissible and persons in lawful custody) is required per certification rules *(CAT.OP.MPA.155* and related *CAT.GEN.MPA.105* and *AMC2 CAT.OP.MPA.165 (f))*	CAs generally have process in place to verify procedures of carriage of special categories of passengers as they shall be reflected in OM A 8.2.2 (a). In the scope related to security this is however not consistently assessed as a part of the certification activity done by the organisational unit competent for AOC certification and requires coordination with security domain.	Some special categories of passengers are defined as “potentially disruptive” and relate to deportees, inadmissible and persons in lawful custody and as such also required to be described in the AOSP.	Typically assessed by both safety and security responsible authority.
Emergency procedures and planning **Alerting ATC to emergencies**	Assessment of security related component is required per certification rules (ORO.MLR.100)	CAs generally have process in place to verify emergency procedures. This is generally covered as a part of the certification activity done by the organisational unit competent for AOC certification and not	Emergency situations refer to non-security and security related and are usually described in Part B (for emergency procedures) and Part D of the Operations Manual. There is typically also separate Emergency Response Plan document in the documentation structure of the air operator.	Typically assessed by both safety and security responsible authority.

Considered element	Security vs certification	General description of the assessment	Description of the nature of relationship with security	Security type of assessment
		focused specifically on security. Due to the security context it requires coordination with security domain.	Additionally, procedures for security emergencies are typically required in the AOSP, however there is no clear regulatory requirement in Regulation 300/2008 for the air operator to have specific emergency procedures related to security	
Information and data security management Protection of electronic and computer systems to prevent intentional and non-intentional system interference and corruption	Assessment of security related component will be required per certification rules (ORO.GEN.200A)	CAs are in the process of establishing a system which would enable assessment of these requirements.	There is a relationship with regulatory aviation security framework related to Annex 17 and EU provisions contained in the Regulation 2015/1998	Typically not assessed during the certification at the moment of developing this report.

In the context of the relationship between the AOSP and OM it would seem important to mention the provision related to the description of OM A section 10 as provided in the AMC3 ORO.MLR.100: "*Security instructions, guidance, procedures, training and responsibilities, taking into account Regulation (EC) No 300/2008. Some parts of the security instructions and guidance may be kept confidential*."

Additionally, AMC1 ORO.AOC.100(a) requires the air operator applying for CAT to provide the AOSP to the Competent Authority. There is, however no clear indication of the purpose of this submission and it is unclear whether this is for the purpose of approval, or just to evidence the document exists and has been already approved.

This seems to be one of the examples where, as indicated earlier in the report D-3.2.1 *"security elements often lack the same depth of guidance or are not available to safety domain (e.g. due to the restricted nature of aviation security regulations)"* and *"the relationship between safety and security is acknowledged within the regulatory frameworks, this recognition often remains declaratory rather than substantive. There is a noticeable absence of comprehensive guidance material that would effectively bridge the two domains, enabling a more integrated approach to certification".*[12]

5.3. Gaps

Interviewees feedback did not highlight specific gaps in most cases. Still, some stakeholders were able to identify aspects they considered worth analysing for future improvements. These included:

- Limited visibility or awareness of security critical elements within safety domain caused either by insufficient information exchange or confidentiality of security information
- Lack of Change management concept in security domain
- Insufficient integration of risk assessment methodologies
- Disharmonised regulatory framework resulting potentially in not fully standardised approach of evaluation
- Unclear impact of severe findings detected by security assessments on certification of aerodromes and air operators (except when security certification is conducted as a separate process)

Furthermore, the analysis of information gathered suggests that separate assessments (of manuals and later during the onsite evaluation) ensures in-depth review and verification of compliance with respective requirements, however it creates the potential gap where security arrangements are analysed without sufficient consideration to safety requirements and some relationships may remain unknown. The research results illustrate more interdependencies between safety and security in the certification process of air operators. This explains the survey data in terms of:

- AOSP needs to be submitted as part of the AOC application
- Link between security non-conformities rectification requirement to complete the AOC process
- Consequences of deficiencies in security on the continuity of the AOC

For aerodromes / airports the distinction between Aerodrome Manual and ASP is clearer as they are more separated in nature and therefore independent.

However separated safety certification is from the evaluation of security, both topics need to be managed typically by the same operator (entity) be it airport operator or air operator and this would be reflected in organisational arrangements. This topic is more extensively described in safety compared to security, especially

[12] Section 9 of the report D-3.2.1

in terms of the concept of Accountable Manager compared to Security Manager and the more general basic concept of SMS compared to SeMS.

In this context the research explored (as indicated on D-3.2.1) if elements commonly recognised through SMS related to organisation and management have any bearing on national practices related to security management and organisation evaluation of aerodromes (airport) and air operators. Elements selected, which are conceptually also included in SeMS, cover:

- Accountability
- Responsibilities
- Security policy

The feedback shows that during the certification process these elements are not assessed in the scope of security (unless it is a separate security certification), in a manner that would allow for consistent and harmonised evaluation of organisational security posture of air operators or airports.

Currently, the accountability concept is not regulated at the EU level in the security domain, meaning the assessment of the Security Program would be restricted to the indication of the position responsible for security without the evaluation, how it correlates with the entire structure and decision-making process in the air operator or airport organisation. As a consequence, the responsibility might be misplaced in a way that it becomes ineffective and cannot influence the organisation to reach the desired level of security and as such may affect compliance.

Considering the intertwined character of safety and security and the already existing framework, organisation and management terms of SMS and ISMS could be leveraged and considered for security.[13]

Additionally, several potential inconsistencies or gaps were revealed during the analysis in the scope of aerodromes certification:

- Change management process is not evaluated in security domain (including impact security measures may have on safety)
- There is very limited interaction in evaluation of security and safety aspect of risk assessments (and consequently related reporting)
- No harmonised approach created to link the airport operator security requirements and aerodrome operator obligations even if this typically is the same organisation
- Most overlapping area between safety and security related to access to the movement area is missing consistent approach (for example airport identification cards or background checks are not included in certification rules related to the access to the movement area)

For aerodromes, the infrastructure elements interlinked with security are related to airside access only (movement area plus the access roads) and cover items like fencing or lighting. However, when assessed by the organisational unit responsible for aerodromes certification they are evaluated from the safety or overall system perspective only and focus mostly on the wild-life prevention. Strong collaboration with the security domain needs to be established to ensure a comprehensive assessment.

- Security requirements are not considered in training certification rules.

Training requirements for subcontractors (ground personnel) should be clarified as it appears to be a gap both for airports and air operators. For example, screeners are not operating in the aerodrome area so they are not covered by training requirements described in the aerodrome certification framework, they are however covered by the airport security regulations. This may cause the situation where an aerodrome is certified but

[13] Best industry practices could be considered, for example IOSA Standards which require air operators to implement SeMS.

may not operate as an airport from the security conformity perspective. Additionally, there is potentially limited or no impact on the continuity of aerodrome certification if there are major and critical deficiencies in their training or performance.

In terms of air operators' certification, inconsistencies or gaps that were revealed during the analysis include:

- Aircraft search – confusion between aircraft search or check per Annex 17 4.3.1 and aircraft search per annex 6, 13.[13]
- Vetting – not included in the qualifications criteria for air operators crew members
- Training of air operator and subcontracted personnel – insufficient or inaccurate guidance in EASA documentation

Air operators typically have management system arrangements which are more integrated due to not only SMS requirements but also industry standards (IOSA). While aerodrome operators seem to prefer the separation model (following the authority) some operators are moving into the direction of air operators recognising system level advantages.

The research also suggests that drafted ground handling regulation should be analysed for security context of the relationship between aerodrome operators and air operators to ensure unintentional gaps are not created. It is important to mention that ground handling entities are not required to have a Security Program unless they are subject to approval for specific regulated security functions. Otherwise ground handlers will typically act as air operators' subcontractors (external service providers) and as such be bound by these operators' instructions.

Finally, and in terms of EASA the research revealed:

- EASA AOC certification guidance does not include elements related to security or any indication about the AOSP[14]
- EASA certification regulation should be reviewed for accuracy and to provide improved AMC especially on topics related to security and where it refers to aviation security regulation implementing acts (Regulation 2015/1998, instead of Regulation 300/2008)
- The topic of third-country oversight – should be reviewed in terms of interdependencies with nationally approved AOSP

5.4. Best practices

Best practices, as suggested by stakeholders, emphasise the importance of enhancing and sustaining coordination and collaboration between the safety and security domains. This is particularly critical in the certification of aerodromes, where security conformity should be integrated into the certification process (unless there is a separate security certification).

Building cross-domain awareness and fostering communication are also essential. Integrated training programs, cross-representation in committees, and other initiatives can help bridge the understanding of how regulations in one domain impact conditions in the other. These measures support prioritisation and decision-making across both safety and security sectors.

[14] easa.europa.eu/sites/default/files/dfu/Leaflet_EASA_AOC_-_5_phases_to_an_AOC.v3.pdf and https://www.easa.europa.eu/en/domains/air-operations/air-operator-certificate-aoc

The implementation of a change management concept within the security domain, alongside the foundational principles of SeMS, is another key recommendation.[15] These principles, already reflected in the Safety Management Systems (SMS) and Information Security Management System (ISMS) under Part-IS regulations, ensure a holistic approach to managing changes and mitigating risks.

Addressing the lack of cross-discipline awareness is essential, and mechanisms should be established to provide safety domain representatives from CAs with access to restricted security information. This access would strengthen their ability to collaborate effectively across disciplines.

A comprehensive methodology for joint working or inspection groups is also recommended. By auditing overlapping areas where feasible, such groups can identify and address findings through joint actions, creating efficiencies and fostering a collaborative culture. Promoting joint awareness activities is equally important to enhance shared principles, improve communication, and build a culture based on common values and priorities.

Integrated or interconnected risk assessments should be developed to reflect shared principles, policies, and processes. For instance, common reporting mechanisms could strengthen these assessments. Furthermore, streamlining and simplifying the regulatory framework is vital. This includes providing comprehensive guidance that clearly delineates safety and security requirements while also highlighting their interdependencies. Areas of overlap should be detailed to ensure a better understanding of how these domains interact. However, integration should not be pursued as a principle in itself. Safety and security have distinct scopes and require specialised expertise. The focus should instead be on creating an environment that offers flexible options and models to benefit organisations, particularly from a management perspective.

In the context of air operators, the complex organisational requirements and extensive documentation they must adhere to should be recognised. Many air operators integrate SMS and Security Management Systems (SeMS), so shared concepts and frameworks must be acknowledged to support their operations effectively.

Finally, the impact of new or modified regulations must be carefully assessed. Coordination mechanisms between safety and security should be in place to ensure regulatory consistency and sensible implementation. This approach would account for all relevant factors, enabling balanced and effective decision-making.

6. Conclusions

This report explored national practices in the assessment of security elements during the certification processes for aerodromes and air operators. The findings highlight several key conclusions regarding the interplay between safety and security and in the context of the report D-3.2.1.

The scope of certification for aerodromes and air operators revealed **insignificant touchpoints with security requirements**. The overwhelming majority of security requirements falls outside of the regulatory certification framework. In the case of aerodromes, safety certification has a limited overlap with the aviation security, largely confined to the requirements related to aerodrome movement area. Security functions, on the other hand, are predominantly managed by airport operators outside this scope. For air operators, the relationship between safety and security is more intertwined, with greater interdependencies influencing certificate issuance and retention. This is because relatively more certification requirements refer to security. Still, most of security requirements applicable to air carriers also falls outside of the certification framework.

[15] Tools available to consider for designing SeMS include for example, EASA Management System Assessment Tool or IATA SeMS Toolkit for External Service Providers

In both cases some States opt for a separate security certification to ensure compliance with broader security regulations. Consequently, typically the certification of aerodromes and air operators and the verification of their conformity with aviation security provisions tend to operate as parallel processes.

Another substantial observation is the **lack of comprehensive guidance at the EU level concerning the overlap** (even if insignificant) **between safety and security requirements** contained in the certification regulatory framework. This gap of insufficient or inaccurate cross-referencing (especially references to security requirements in safety regulations) impacts national processes implemented by Competent Authorities. Mostly currently visible in the subject of air operator crew training and aircraft search/check procedures (see Table 7), may potentially become more concerning if e.g. reporting related to security is outside of the certification regulatory framework.

Furthermore, in terms of management aspect, there are systemic inconsistencies where responsibilities and accountabilities for safety are typically well-defined through models like Accountable Manager and Nominated Persons within Safety Management Systems (SMS), whereas equivalent systemic structures for security are absent or inconsistently implemented. While some national processes assess individuals responsible for security, such as security managers, these efforts are not fully integrated into the overarching certification framework. Similarly, processes related to security reporting and change management remain siloed from their safety counterparts.

The interdependencies between safety and security are further complicated by the absence of comprehensive guidance materials that bridge these domains. Unequal treatment of Safety Management Systems (SMS) and Security Management Systems (SeMS) exemplifies this issue, as does the limited access of safety experts to restricted security guidance. These factors hinder efforts to adopt an integrated approach to certification.

Terminology differences between safety and security domains also impede effective communication and coordination. Aligning terminology would facilitate better understanding and interoperability, particularly for processes that share equivalent goals and outputs.

In conclusion, a more integrated approach to safety and security within the regulatory framework is recommended. Harmonising and aligning these domains would not only improve regulatory compliance but also enhance the overall safety and security of aviation operations. Strengthening coordination, developing comprehensive guidance materials, standardising terminology, and recognising the interdependencies between safety and security are essential steps toward achieving a more effective and unified certification process. Such measures would lead to improved outcomes and a safer, more secure aviation industry.

BIBLIOGRAPHY

ICAO Annex 14 Aerodromes Vol. I – Aerodromes Design and Operations

ICAO Annex 6 Operation of aircraft Part I – International Commercial Air Transport Aeroplanes

ICAO Annex 17 Aviation Security

Regulation (EU) 2018/1139 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Commission Regulation (EU) No 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.

Commission Regulation (EU) No 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures

Adams, W. C. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation*, 492-505.

EASA AOC: to cert or not to cert, February 2021 - https://www.lexology.com/library/detail.aspx?g=bb8f7b52-d59e-4867-a9e9-dc42af128566

Reporting of Aviation Security Occurrences and Incidents, ICAO, June 2022 - https://www.icao.int/Security/SFP/Pages/Incident-Reporting-Guidance-and-Taxonomy.aspx

EASA Management System Assessment Tool, September 2023 - https://www.easa.europa.eu/en/document-library/general-publications/management-system-assessment-tool

IATA Security Management System Toolkit for External Service Providers, September 2024

Methodologies and Approaches to Managing Interacting Aviation Risks, Working Paper (AN-Conf/14-WP/56), 14th ICAO Air Navigation Conference, 2024 - https://www.icao.int/Meetings/anconf14/Pages/default.aspx

APPENDIX

Certification terms below is referred to here as a process based on the Regulation 139/2014 for aerodromes and Regulation 965/2012 for air operators. Interviews indicated some States may have nationally established specific security certification process for an airport and air operators.

INTERVIEW ANSWERS COVERING AERODROMES CERTIFICATION

Topic	Aerodrome 1	Aerodrome 2	Aerodrome 3	Aerodrome 4	Aerodrome 5	Aerodrome 6	Aerodrome 7	Aerodrome 8	Aerodrome 9	Aerodrome 10	Aerodrome 11	Aerodrome 12	Aerodrome 13	Aerodrome 14	Aerodrome 15
Security consideration in certification	There is organizational separation at the airport and Authority level The area where security is considered is: • in relation to infrastructure changes (e.g. the layout of the SRA or fence) and only if initiated by safety .	There is organizational separation at the airport and Authority level The only area where security is considered is: • preventing unauthorized people from coming into the airside of an aerodrome	There is organizational separation at the airport and Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the airport and Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the airport and Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level The area where security is considered is: • fence	There is organizational separation at the airport and Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level No direct security considered in the certification of an aerodrome.	There is organizational separation at the airport and Authority level The area where security is considered is: • the construction of new or alteration of existing infrastructure	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.	There is organizational separation at the Authority level Security elements are not considered specifically in the certification of an aerodrome.
Desired security requirements in certification	Due to the specificity of security domain it is desirable to maintain separation.	Due to the specificity of security domain it is desirable to maintain separation.	No specific suggestions	Certification should consider the following security elements: • security training • security reporting • aerodrome boundaries, fence, CCTV system or patrolling of access to the area inside the fence	Including security conceptually appears natural because how can one feel safe when having security issues? However, there is a greater risk of additional administrative burden and duplication of work.	Certification framework should be more flexible, allowing to use synergies in resource management at the airport level.	Overlapping elements (e.g. fence) could be more integrated. Additional material similar to the AMC part of EASA would be valuable	Very difficult to determine due to classified nature of all security information and lack of access to them by the safety domain.	No specific suggestions	Overlapping elements (e.g. related to infrastructure) could be more integrated.	No specific suggestions	No specific suggestions	No specific suggestions	No specific suggestions	Certification should consider the following security elements: • perimeter fencing • requirements, lighting of the apron • contingency and response procedures, safety/security tests or exercises
Preferred certification audit approach	Preferred as separate processes due to: • substantial differences between safety and security domain	Preferred as separate processes due to: • organisational arrangements at the Authority level	Preferred as separate processes due to: • specifics and granularity of assessments in either domain	Preferred as combined into one process as synchronization may result in more efficiency and improved resolution of findings. It could also bolster the	Preferred as separate process as administrative burden is already large enough. However, overlapping areas could benefit from	Preferred as combined into one process as it is reflecting of increasing integrated approach.	Preferred as combined into one process as there are similarities in the processes and this could help in applying same methodology.	Preferred as separate processes due to: • very different nature in the core of two concepts, especially in relation to confidential	Preferred as separate processes due to: • largely different scope (safety – airside, security – terminal) with coordination in relation to overlapping areas of interest	Preferred as separate process due to: • substantial differences also in relation to confidential nature of security. However, overlapping	Preferred as separate processes due to: • substantial differences between safety and security domain, specific expertise required and	Preferred as separate processes due to: • different scope and logistic arrangements	Preferred as separate processes due to: organisational arrangements at the Authority level and differences in conformity assessment methodology	Preferred as separate processes (as it currently works)	Preferred as separate processes with coordination mechanisms in place when needed

Topic	Aerodrome 1	Aerodrome 2	Aerodrome 3	Aerodrome 4	Aerodrome 5	Aerodrome 6	Aerodrome 7	Aerodrome 8	Aerodrome 9	Aerodrome 10	Aerodrome 11	Aerodrome 12	Aerodrome 13	Aerodrome 14	Aerodrome 15
				cross-domain understanding.	improved coordination.			nature of security		areas (infrastructure) could benefit from improved coordination expertise.	confidential nature of security				
Challenges in managing safety and security in certification process	No	Overwhelming regulations in both domains Information sharing between safety and security	No	Certification framework does not mention specifically security as a part of Change management	No	Regulation in either domain has a very different structure and terminology. Security regulation should be more risk-based.	High degree of disconnect between safety and security visible e.g. through the separation of safety and security training	No	No	Upcoming challenge related to Part-IS Security does not apply the same Change management and there is much less flexibility when applying the regulation Regulatory framework is very specific	No	No	No	Challenges related to cases where serious findings are detected against aviation security requirements (based on the NCASP) and if the rectification how is formally linked to the certification of aerodrome process	General challenge in terms of security elements linked to safety (drones, cyber, contingency and response plan procedures etc.)
Personnel familiarity with safety and security	Good level of understanding of respective requirements	Good level of understanding of respective requirements	General level of understanding of respective requirements	Basic level of understanding of respective requirements	Low level of understanding of respective requirements	High level of understanding of respective requirements	Basic level of understanding of respective requirements	Basic level of understanding of respective requirements	Low level of understanding of respective requirements	General level of understanding of respective requirements	Low level of understanding of security requirements in safety domain Basic level of understanding of safety requirements in security domain	Basic level of understanding of respective requirements	General level of understanding of respective requirements	Basic level of understanding of respective requirements	Basic level of understanding of respective requirements
Safety and security process alignment	Preferred separation of safety and security processes (as it is currently)	Preferred separation of safety and security processes (as it is currently) However, information sharing between domains would be beneficial.	Preferred separation of safety and security processes (as it is currently) However, information sharing between domains would be beneficial.	Preferred more synchronization of safety and security processes Integration between domains would result in efficiencies and be beneficial as an event on one side can impact other domain	Depending on the topic / identified effectiveness / efficiency: could be either more synchronized or more separate.	Preferred more synchronization of safety and security processes Increased coordination would benefit both safety and security	Preferred more synchronization of safety and security processes Especially concerning methodology, handling of findings, change management	Preferred separation of safety and security processes (as it is currently)	Preferred separation of safety and security processes (for conformity assessment) However, regulatory elements and conformity assessment methodology could be better aligned to avoid potential issues.	Preferred separation of safety and security processes (as it is currently - especially in terms of procedures) However, some elements, e.g. emergency response planning could benefit from the improved coordination.	Preferred separation of safety and security processes (as it is currently) However, more convergence on some points (SMS/SeMS, risk management, security reporting) and more coordination to achieve mindset alignment would be beneficial.	Preferred separation of safety and security processes (as it is currently)	Preferred separation of safety and security processes (as it is currently) However, information sharing between domains would be however beneficial	Preferred more synchronization of safety and security processes	Preferred separation of safety and security processes (as it is currently) However, coordination mechanisms should be in place when needed.
Gaps in safety-	No gaps identified	No gaps identified	No gaps identified	Due to separation there is very	No gaps identified	Disharmonised regulatory framework	Disconnect between domains caused	Disconnect between domains	Disconnect between domains caused by	No formalised impact assessment as	No gaps identified	No gaps identified	Some overlaps due to certification of	No gaps identified	Ensuring that all elements of risk methodologies

Topic	Aerodrome 1	Aerodrome 2	Aerodrome 3	Aerodrome 4	Aerodrome 5	Aerodrome 6	Aerodrome 7	Aerodrome 8	Aerodrome 9	Aerodrome 10	Aerodrome 11	Aerodrome 12	Aerodrome 13	Aerodrome 14	Aerodrome 15
security certification				limited visibility of security critical elements in safety.			by confidentiality in security	caused by confidentiality in security	confidentiality in security Organisation of security oversight is lagging compared to safety oversight	part of Change management, when security measures are modified but without assessing safety outcomes			aerodromes and ground handling, especially for airports providing for handling as one organization		integrate safety and security aspects
Best practices for safety-security coordination	Generally encouraged collaboration between the two domains Potentially more consideration to culture and just culture in particular in security Security domain does not have a process to initiate Change management when amending the ASP, maybe something to consider Good security helps safety.	Develop and maintain information exchange to increase mutual understanding Guidance related to links between EASA regulations and security impact would be helpful also in terms of encouraging *Change management* approach in security	Develop and maintain communication channels Perhaps raising awareness of mutual influence between safety and security. Guidance material might be helpful but is not necessary. Security should apply same Change management process	Develop and maintain information exchange to increase mutual understanding Promote integrated Management Systems approach According to SMS every process should trigger Change Management so security should be part of it too.	Promote cross-sectoral knowledge sharing by creating joint working / inspection groups Security should be more integrated in the certification to have a more comprehensive resolution of findings but only where it is beneficial and does not create additional burden	Improve harmonization of regulatory framework Research of other industries to identify best practices for safety and security management models EASA to develop guidance on management system The operator applies a very centralized and coordinated approach under one Management scheme which incorporates both, safety and security. By applying the process approach e.g. *Change management* is integrated in the security management practices.	Alignment of methodologies for compliance assessment, change management, reporting. Integration of management methods and more efficient utilisation of resources Risk-based approach should be encouraged in security domain as this would allow to adjust arrangements based on the local situation of the individual airport	Streamline and simplify aerodromes certification framework which is becoming too broad in scope and complex comparing to typical safety scope Promote common change management approach	Improve coordination and harmonization of regulatory framework Development of guidance to show interdependencies with security Introduce integrated approach towards management systems including security Promote safety oversight model in security domain Information exchange between departments of the Authority ensures security arrangements are in place when the certificate is issued. More clear provisions could assist to ensure security requirements are considered when developing safety measures and vice versa.	Develop and maintain information exchange to increase mutual understanding Build awareness trough cross-domain training and familiarisation Security shall consider Change management process Change management should be considered, when security measures are modified Deeper collaboration will be required in terms of Part –IS implementation	Develop and maintain information exchange to increase mutual understanding Areas where safety and security overlaps will be checked by either certification process independently and coordinated at the Authority level.	Develop and maintain information exchange to increase mutual understanding Cross-domain representation in committees / groups Including safety personnel in vetting process to allow them access to security information Merging safety and security training to facilitate airport processes Areas where safety and security overlaps will be checked independently and coordinated at the Authority level	Develop and maintain information exchange to increase mutual understanding Equip safety domain as necessary with credentials / security clearance to allow access to security sensitive information Areas where safety and security overlap will be checked independently and coordinated at the Authority level	Initial meeting with the applicant so different requirements (safety and security) are explained Areas where safety and security overlaps will be checked independently and coordinated at the Authority level.	Strengthening processes of: • Impact assessment of new and/or modified regulations • Integrated risk management • security occurrence reporting system

INTERVIEW ANSWERS COVERING AIR OPERATOR'S CERTIFICATION

Topic	Air Operator 1	Air Operator 2	Air Operator 3	Air Operator 4	Air Operator 5	Air Operator 6	Air Operator 7	Air Operator 8	Air Operator 9	Air Operator 10
Security consideration in certification	There is organizational separation at the Authority level Security certification of air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level Security certification of air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process	There is organizational separation at the Authority level AOSP assessment process for air operators is a separate process
Desired security requirements in certification	Enhanced system approach and integration similarly to operator arrangements	No specific suggestions	Security should be included as a part of management / organization arrangements	Information security should be included	No specific suggestions	No specific suggestions	No specific suggestions	No specific suggestions	No specific suggestions	Safety requirements should be verified first. Once this phase is completed the next step would be an assessment of security conformity.
Preferred certification audit approach	Combined approach where organizational process could be merged (documentation, risk analysis, reporting etc.) because of integration at the air operator level. This could be followed by two separate processes of evaluation of operational elements.	Preferred as separate due to: • specifics and granularity of assessments in either domain combined with necessary expertise	Preferred as combined into one process as it is reflective of the integrated approach	Preferred as separate due to: • specifics and granularity of assessments in either domain combined with necessary expertise	Preferred as separate due to: • specifics and granularity of assessments in either domain combined with necessary expertise	Preferred as separate processes due to: • substantial differences between safety and security domain, specific expertise required and confidential nature of security	Preferred as separate processes due to: • different scope and logistic arrangements	Preferred as separate processes due to: • organisational arrangements at the Authority level and differences in conformity assessment methodology	Preferred as separate processes (as it currently works)	Preferred as separate processes with coordination mechanisms in place when needed
Challenges in managing safety and security	Security conformity assessments do not take into account broader context of regulatory environment applicable to air operators and it specifics. This results in challenge to manage operational documentation.	No	Lack of clarity in the regulation. In terms of management of different manuals, the air operator ensures coordination of content (for example OM A Chapter 10) as this is reasonable and also important for IOSA audit. This approach is however not shared by the authority.	Confidentiality of security information. Information security is a very complex topic	The language of OM A Chapter 10 is sometime not reflective of security terminology causing difficulties in assessment of this part	Coordination of activities between safety and security.	Internal challenge is resources of qualified personnel given increasing number of AOC	Issues with oversight of "group operations" in the safety domain and it may become also an issue for security oversight including for the AOSP approval.	Challenge relates to the need for in-depth analysis of many operation manuals to extract security content for evaluation. This is related to complexity of documentation and documentation management.	General challenge in terms of security elements linked to safety as drones, cyber, contingency and response plan procedures etc.
Personnel familiarity with safety and security	Considerable level of understanding of respective requirements	Considerable level of understanding of respective requirements	Considerable level of understanding of respective requirements	General level of understanding of respective requirements	Low level of understanding of security requirements in safety domain	Low level of understanding of security requirements in safety domain Basic level of understanding of safety requirements in security domain	Basic level of understanding of respective requirements	General level of understanding of respective requirements	Basic level of understanding of respective requirements	Basic level of understanding of respective requirements
Safety and security process alignment	Preferred more synchronization of safety and security processes as it would increase the efficiency (especially for the processes that overlap)	Preferred separation of safety and security due to depth of subject expertise required However, it would be welcomed if	Preferred more synchronization of safety and security processes	Preferred more synchronization of safety and security processes However, this would result in the need to expand personnel competences into both domains.	Preferred separation of safety and security due to competences assigned at the Authority level However, more integration could result in additional coordination difficulties.	Preferred separation of safety and security processes (as it is currently) More convergence on some points (SMS/SeMS, risk management, security reporting)	Preferred separation of safety and security processes (as it is currently)	Preferred separation of safety and security processes (as it is currently) However, information sharing between domains would be however beneficial.	Preferred more synchronization of safety and security processes	Preferred separation of safety and security processes (as it is currently) However, coordination mechanisms should be in place when needed.

Topic	Air Operator 1	Air Operator 2	Air Operator 3	Air Operator 4	Air Operator 5	Air Operator 6	Air Operator 7	Air Operator 8	Air Operator 9	Air Operator 10
		overlapping areas are synchronized				and more coordination to achieve mindset alignment				
Gaps in safety-security certification	Security Management System (SeMS) is not included	No	Not fully standardized approach between different regulators Lack of clarity in the scope of information security	Lack of clarity in the scope of information security	No	No	No	No	No	Ensuring that all elements of risk methodologies integrate safety and security aspects
Best practices for safety-security coordination	Preferred if there is one audit covering both domains so that the potential rectification of findings is improved	Coordination of processes that overlap between safety and security	Use of system-approach (similar to IOSA model which seems to work) Cooperation related to the implementation of new regulations e.g. Part-IS Security should be managed the same as safety, so there should be same Accountable Manager	Promotion and building awareness of safety and security as intertwined and to improve exchange of information between these two domains	Develop and maintain communication channels	Develop and maintain information exchange to increase mutual understanding	Develop and maintain information exchange to increase mutual understanding Cross-domain representation in committees / groups Including safety personnel in vetting process to allow them access to security information Merging safety and security training to facilitate processes	Develop and maintain information exchange to increase mutual understanding Equip safety domain as necessary with credentials / security clearance to allow access to security sensitive information	Initial meeting with the applicant so different requirements (safety and security) are explained	Strengthening processes of: • Impact assessment of new and/or modified regulations • Integrated risk management • Security occurrence reporting system

European Union Aviation Safety Agency

Konrad-Adenauer-Ufer 3
50668 Cologne
Germany

Mail EASA.research@easa.europa.eu
Web www.easa.europa.eu

An Agency of the European Union