



# EUROCONTROL Guidelines for the Oversight of Air Traffic Management Security

Edition number: 1.0  
Edition date: 11/11/2022  
Document reference: EUROCONTROL-GUID-191





# **EUROCONTROL Guidelines for the Oversight of Air Traffic Management Security**

**DOCUMENT IDENTIFIER : EUROCONTROL-GUID-191**

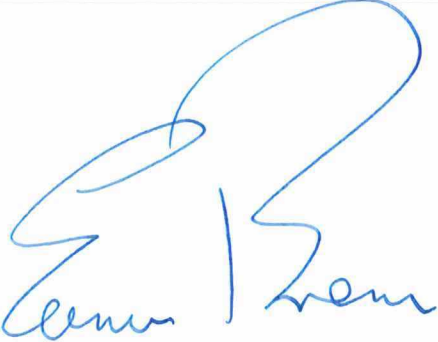
<b>Edition Number:</b>	<b>1.0</b>
<b>Edition Date :</b>	<b>11/11/2022</b>
<b>Status :</b>	<b>Released Issue</b>
<b>Intended for :</b>	<b>General Public</b>
<b>Category :</b>	<b>EUROCONTROL Guidelines</b>

## DOCUMENT CHARACTERISTICS

TITLE			
<b>EUROCONTROL Guidelines for the Oversight of Air Traffic Management Security</b>			
<b>Publications Reference:</b> GUID-191			
<b>ISBN Number:</b> 978-2-87497-121-1			
<b>Document Identifier</b>	<b>Edition Number:</b> 1.0		
EUROCONTROL-GUID-191	<b>Edition Date:</b> 11/11/2022		
Abstract			
<p>This document supports national authorities responsible for ATM security oversight, namely the Appropriate Authorities (AA) in the context of ICAO, and the National Supervisory Authorities (NSA) in the context of the Single European Sky (SES). Effective oversight should facilitate the development of a harmonised level of security across States and between organisations, enhancing mutual trust between stakeholders in the process.</p> <p>These guidelines document a process to support NSAs in performing security oversight activities.</p> <p>Regulatory requirements and guidance material are analysed to provide examples of the development of audit check-lists for NSA, and self-assessment questionnaires for entities subject to oversight. The necessary skill requirements of Audit Team members are also presented.</p>			
Keywords			
Security Oversight	Oversight Process	Compliance	Security Regulation
National Supervisory Authorities	Audit check-lists	Self-assessment questionnaire	Audit team skills
Contact Person(s)		E-mail	
John Hird		standardisation@eurocontrol.int	

STATUS, AUDIENCE AND ACCESSIBILITY					
Status	Intended for		Accessible via		
Working Draft	<input type="checkbox"/>	General Public	<input checked="" type="checkbox"/>	Intranet	<input type="checkbox"/>
Draft	<input type="checkbox"/>	EUROCONTROL	<input type="checkbox"/>	Extranet	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/>	Restricted	<input type="checkbox"/>	Internet (www.eurocontrol.int)	<input checked="" type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>				

# DOCUMENT APPROVAL

AUTHORITY	NAME AND SIGNATURE	DATE
Director General	 Eamonn BRENNAN	11/11/22.



## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	11/11/2022	Document creation, supersedes former EUROCONTROL "Manual for National Security Oversight"	All

# CONTENTS

<b>DOCUMENT CHARACTERISTICS</b> .....	<b>2</b>
<b>DOCUMENT APPROVAL</b> .....	<b>3</b>
<b>DOCUMENT CHANGE RECORD</b> .....	<b>4</b>
<b>CONTENTS</b> .....	<b>5</b>
<b>LIST OF FIGURES</b> .....	<b>7</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>9</b>
<b>1. Introduction</b> .....	<b>10</b>
1.1 Purpose of the document .....	10
1.2 EUROCONTROL Guidelines .....	10
1.3 Structure of the document.....	10
1.4 Applicability .....	11
1.5 Maintenance of the Specification .....	11
1.6 Scope .....	11
1.7 Definitions.....	12
1.8 Abbreviations .....	12
1.9 Reference material .....	14
<b>2. ATM Security Oversight</b> .....	<b>16</b>
2.1 Overview .....	16
2.2 Applicable Rules and Regulations .....	16
2.2.1 Global .....	16
2.2.2 The European Region.....	18
2.2.3 Regulatory Complexity.....	19
2.2.4 Harmonisation .....	20
2.3 Assumptions .....	20
<b>3. Guidance for ATM Security Oversight</b> .....	<b>21</b>
3.1 The Oversight Programme.....	21
3.1.1 ICAO Security Monitoring Activities.....	21
3.1.2 SES ATM Security Regulatory Requirements.....	21
3.2 Recommended Oversight Process .....	23
3.3 Actors.....	23
3.3.1 Competent Authority .....	23
3.3.2 Audit Team .....	24
3.3.3 Service Provider .....	24
3.4 Systems and Tools.....	25
3.5 Controls and Checks.....	26

3.6	Risks .....	26
3.7	Opportunities.....	26
3.8	Performance Indicators .....	26
3.9	Inputs .....	27
3.10	Outputs .....	27
4.	Process Steps.....	28
4.1	Start Point.....	28
4.2	Initiation .....	28
4.3	Preparation .....	33
4.4	Execution.....	33
4.5	Reporting .....	34
4.6	Follow-Up.....	36
4.7	Closure.....	37
4.8	End Point .....	37
5.	Conclusions.....	38
	ANNEX A – Document Update Procedures .....	39
	ANNEX B – Security Monitoring .....	40
	ANNEX C – Compliance Classification Schemes .....	41
	C.1 ICAO Doc 8973.....	41
	C.2 Regulation (EC) 72/2010.....	41
	C.3 Security Compliance Classification Scheme Mapping.....	42
	C.4 Regulation (EU) 2017/373 Compliance Classification Scheme .....	43
	ANNEX D – Document Summaries .....	45
	D.1 ICAO .....	45
	D.2 European Region.....	47
	ANNEX E – Applicable Requirements and Audit Team Skills.....	50
	E.1 ATM/ANS.OR.B.005 Management system .....	50
	E.2 ATM/ANS.OR.D.010 Security management .....	52
	E.3 ATM/ANS.OR.B.020 Personnel requirements.....	54
	E.4 ATM/ANS.OR.A.070 Contingency Plans .....	54
	E.5 ATSEP.OR.105 Training and competence assessment programme.....	55
	ANNEX F – Process Documents.....	56
	ANNEX G – Mapping of ATM/ANS.OR.D010 to Guidance Material .....	58
	ANNEX H – Check-list / Self-assessment Example.....	64

## LIST OF FIGURES

Figure 1 – Regulations and Guidance Material.....	19
Figure 2 – Security Requirements from Regulation (EU) 2017/373 .....	22
Figure 3 – EASA eRules Colour Coding.....	25
Figure 4 - Oversight Process Turtle Diagram.....	30
Figure 5 – Oversight Process (Part 1) .....	31
Figure 6 – Oversight Process (Part 2) .....	32

## LIST OF TABLES

Table 1 – Critical Elements for Security Oversight.....	17
Table 2 – Initiation Steps .....	29
Table 3 – Preparation Steps .....	33
Table 4 – Execution Steps .....	34
Table 5 – Regulation (EU) 2017/373 Compliance Classification Scheme.....	35
Table 6 – Reporting Steps .....	35
Table 7 – Follow-up Steps .....	36
Table 8 – Closure Steps.....	37
Table 9 - Types of Monitoring Activities.....	40
Table 10 – ICAO Doc 8973 – Compliance Classification Scheme.....	41
Table 11 – Regulation (EC) 72/2010 – Compliance Classification Scheme .....	42
Table 12 – Compliance Classification Scheme – Possible Mapping .....	43
Table 13 – Regulation (EU) 2017/373 - Compliance Classification Scheme.....	43
Table 14 – ICAO Document Summaries .....	46
Table 15 – Summary of EU Legislation and European Regional Documents .....	49
Table 16 - ATM/ANS.OR.B.005 Management system.....	52
Table 17 - ATM/ANS.OR.D.010 Security management.....	53
Table 18 - ATM/ANS.OR.B.020 Personnel requirement.....	54
Table 19 - ATM/ANS.OR.A.070 Contingency Plans.....	54
Table 20 – ATSEP.OR.105 Training and competence assessment programme .....	55
Table 21 – Oversight Process Documents .....	57
Table 22 – Example Mapping of ATM/ANS.OR.D.010 to Guidance Material.....	63
Table 23 – Example Table for Checklists or Self-assessment .....	68





## EXECUTIVE SUMMARY

This document, the “EUROCONTROL Guidelines for the Oversight of Air Traffic Management Security” supersedes the EUROCONTROL “Manual for National Security Oversight”, which was first released in 2012, and updated in 2013 [RD 1].

These guidelines have been developed in response to changes in the regulatory framework since the release of Edition 2.0, which include the release of the Network and Information Security Directive [RD 15], the update to the common requirements [RD 8], and the publication of the Cybersecurity Act [RD 13].

This document supports national authorities responsible for ATM security oversight, namely the Appropriate Authorities (AA) in the context of ICAO, and the National Supervisory Authorities (NSA) in the context of the Single European Sky (SES).

Security oversight is a State responsibility and an enabler to support the resilience of the aviation system to acts of unlawful interference. The oversight process seeks to verify the compliance of service providers with the regulatory framework, to identify areas for improvement, and to support enhancements to the security posture of the aviation system.

Effective oversight should facilitate the development of a harmonised level of security across States and between organisations, enhancing mutual trust between stakeholders in the process.

Within the State, it is the responsibility of the NSA to perform ATM security oversight activities, which include the following tasks:

- carrying out security inspections on ANSPs; and
- monitoring the implementation of applicable regulations and implementing rules by the national aviation authorities, subject to EASA standardisation inspections.

These guidelines document a process to support NSAs in performing security oversight activities.

Regulatory requirements and guidance material are analysed to provide examples of the development of audit check-lists for NSA, and self-assessment questionnaires for entities subject to oversight. The necessary skill requirements of Audit Team members are also presented.

# 1. Introduction

This document provides EUROCONTROL Guidelines for Air Traffic Management Security Oversight.

Security oversight is a compliance monitoring and verification process by which security authorities obtain evidence that the required and expected security performance is met by different stakeholders in the Air Traffic Management (ATM) system.

Oversight requirements are described in ICAO SARPS (Standards and Recommended Practices) and guidance material, and in EU regulations and directives. The applicable publications are presented in section 2.2.

## 1.1 Purpose of the document

The purpose of this document is to provide guidance on how an NSA, acting as a Competent Authority, can perform the security oversight of an Air Navigation Service Provider (ANSP).

This guidance document supersedes the EUROCONTROL “Manual for National Security Oversight”, which was originally released in 2012 and updated in 2013 [RD 1].

These guidelines describe the current regulatory environment and recommend a process to support NSAs in performing ATM Security oversight activities. It is assumed that the State has developed an aviation security policy and associated regulations, standards, measures, practices and procedures, which is reflected in the National Civil Aviation Security Programme (NCASP).

## 1.2 EUROCONTROL Guidelines

EUROCONTROL Guidelines, as defined in the EUROCONTROL Regulatory and Advisory Framework (ERAF), are advisory and contain:

*“Any information or provisions for physical characteristic, configuration, material, performance, personnel or procedure, the use of which is recognised as contributing to the establishment and operation of safe and efficient systems and services related to ATM in the EUROCONTROL Member States”.*

The application of EUROCONTROL Guidelines is optional.

The EUROCONTROL Regulatory and Advisory Framework (ERAF) also specifies that:

*“EUROCONTROL Guidelines may be used inter alia to support implementation and operation of ATM systems and services, and to:*

- *complement EUROCONTROL Rules and Specifications;*
- *complement ICAO Recommended Practices and Procedures;*
- *complement EU legislation;*
- *indicate harmonisation targets for ATM Procedures;*
- *encourage the application of best practice;*
- *provide detailed procedural information.”*

## 1.3 Structure of the document

The document comprises the following chapters:

- a) Section 2 describes the context for security oversight, addressing global and European regulatory requirements, and summarising the required capabilities of States in this area. The assumptions of the document are also stated.
- b) Section 3 provides guidance on ATM Security Oversight, and includes the following: a description of the type and scope of oversight activities; an overview of a recommended oversight process which may be used (or adapted) for use in training or to guide oversight activities; descriptions of the actors involved, as well as required systems and tools, risks, opportunities, Performance Indicators (PIs) and inputs.
- c) Section 4 describes the steps of the oversight process in detail.
- d) Section 5 concludes the document.
- e) Annex A describes the update procedures for this document.
- f) Annex B describes the types of monitoring activities employed during oversight.
- g) Annex C describes the compliance classification schemes employed by EASA and ICAO.
- h) Annex D contains contextual summaries of applicable regulations and guidance material.
- i) Annex E describes the security requirements imposed on Entities by IR (EU) 2017/373 [RD 8] and its amendments, and the corresponding skills required of the Audit Team.
- j) Annex F provides the required contents of documents produced during the oversight process.
- k) Annex G provides an example of a mapping of security management requirements in IR (EU) 2017/373 [RD 8] to guidance material.
- l) Annex H provides an example of a regulatory requirements checklist / self-assessment table.

## 1.4 Applicability

This document is intended to be read and used by NSAs, or other state appointed Competent Authorities (civil or military) to perform ATM Security oversight activities.

Other stakeholders may be interested in reading the content as a comprehensive overview of ATM Security oversight. These may include Air Navigation Service Providers (ANSPs), Air Traffic Flow Managers, and the Network Manager, in the EUROCONTROL Member States and Comprehensive Agreement States.

## 1.5 Maintenance of the Specification

This EUROCONTROL Specification has been developed under the EUROCONTROL Regulatory and Advisory Framework (ERAF) and is maintained by EUROCONTROL in accordance with this Framework and in line with the EUROCONTROL Standards Development Procedures. The procedures are described in detail in Annex A.

## 1.6 Scope

Security oversight supports security authorities in obtaining evidence that the required and expected security performance is met by stakeholders in the ATM/ANS system. Oversight requirements are described in ICAO SARPS and guidance material, and in EU regulations and directives.

This guidance document focuses on the security-related requirements of Reg. (EU) 2017/373 [RD 8] and its amendments. The main security requirements are contained in the section "ATM/ANS.OR.D.010 Security Management". Other requirements which are related to security, and which may have interdependencies with security are also addressed.

## 1.7 Definitions

Asset	<i>Something that has value to an organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation (ISO 27000:2018 [RD 17])</i>
ATM Security	<i>The contribution of the ATM system to civil aviation security, national security and defence, and law enforcement; and the safeguarding of the ATM system from security threats and vulnerabilities. (ICAO Doc 9985 [RD 5] 3.7)</i>
Control	<i>Measure that is modifying risk. (Note: Controls include any process, policy, device, practice, or other actions which modify risk) (ISO/IEC 27000:2018 [RD 17])</i>
Entity	<i>A public or private organisation involved in implementing aviation security measures, and subject to quality control activities</i>
Impact	<i>The extent to which a loss of confidentiality, availability or integrity of an asset affects the achievement of business objectives, and as an evaluated consequence of a particular event". (ISO/PAS 22399 [RD 18])</i>
Resilience	<i>The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning (NIST SP800-34 [RD 19])</i>
Threat	<i>A potential cause of an unwanted incident which could result in harm to a system or function (ISO/IEC 27000:2018 [RD 17])</i>
Vulnerability	<i>Weakness of an asset or control that can be exploited by one or more threats. (ISO/IEC 27000:2018 [RD 17])</i>

## 1.8 Abbreviations

AA	Appropriate Authority
AMC	Acceptable Means of Compliance
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSP	Air Traffic Service Provider
AVSEC	AViation SECurity
CA	Competent Authority
CAA	Civil Aviation Authority
CE	Critical Element
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CNS	Communications, Navigation, Surveillance

CSIRT	Computer Security Incident Response Team
EASA	European Union Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
ENISA	European Network and Information Security Agency
FAA	Federal Aviation Administration
GM	Guidance Material
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technologies
NCA	National Competent Authority
NCASC	National Civil Aviation Security Committee
NCASP	National Civil Aviation Security Programme
NCASQCP (or NQCP)	National Civil Aviation Security Quality Control Programme
NCASTP	National Civil Aviation Security Training Programme
NEASCOG	NATO-EUROCONTROL ATM Security Coordinating Group
NIS	Network and Information Security
NM	Network Manager
NSA	National Supervisory Authority
PI	Performance Indicator
SARPs	Standards and Recommended Practices (ICAO)
SeMS	Security Management System
SES	Single European Sky
USAP	Universal Security Audit Programme
USAP-CMA	USAP Continuous Monitoring Approach

## 1.9 Reference material

- [RD 1] EUROCONTROL, *Manual for National ATM Security Oversight*, Edition 2.0, October 2013
- [RD 2] ICAO Annex 17 to the Convention on International Civil Aviation, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Amendment 18, 12<sup>th</sup> Edition, 2022
- [RD 3] ICAO Doc. 8973 (Restricted), *Security Manual for Safeguarding Civil Aviation against acts of Unlawful Interference*, 12th Edition, 2020
- [RD 4] ICAO Doc. 9807, *Universal Security Audit Programme Continuous Monitoring Manual*, 3<sup>rd</sup> Edition, 2021
- [RD 5] ICAO Doc. 9985 (Restricted), *Air Traffic Management Security Manual*, 1st Edition, 2013
- [RD 6] ICAO Doc 10047, “*Aviation Security Oversight Manual – The Establishment and Management of a State’s Aviation Security Oversight System*”, 2<sup>nd</sup> Edition, 2021.
- [RD 7] Regulation (EC) 549/2004, *laying down the framework for the creation of the single European sky*, 10<sup>th</sup> March 2004
- [RD 8] Commission Implementing Regulation (EU) 2017/373, *laying down common requirements for providers of air traffic management / air navigation services and other air traffic management network functions and their oversight ...*, 1<sup>st</sup> March 2017
- [RD 9] Implementing Regulation (EU) 2020/469, *of 14 February 2020 amending Regulation (EU) No 923/2012, Regulation (EU) No 139/2014 and Regulation (EU) 2017/373 as regards requirements for air traffic management/air navigation services, design of airspace structures and data quality, runway safety*, 14<sup>th</sup> February 2020
- [RD 10] Regulation (EC) No 300/2008, *on common rules in the field of civil aviation security*, 11<sup>th</sup> March 2008
- [RD 11] Implementing Regulation (EU) 2015/1998, *laying down detailed measures for the implementation of the common basic standards on aviation security*, 5<sup>th</sup> November 2015
- [RD 12] 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*, 4<sup>th</sup> July 2018
- [RD 13] Regulation (EU) 2019/881, *on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, 17<sup>th</sup> April 2019
- [RD 14] Commission Implementing Regulation (EU) 628/2013, *on working methods of the European Aviation Safety Agency for conducting standardisation inspections...*, 28<sup>th</sup> June 2013
- [RD 15] Directive (EU) 2016/1148, *concerning measures for a high common level of security of network and information systems across the union*, 6<sup>th</sup> July 2016
- [RD 16] Commission Implementing Regulation (EU) 2019/1583, *laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures*, 25<sup>th</sup> September 2019
- [RD 17] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*
- [RD 18] ISO/PAS 22399:2007, *Societal security - Guideline for incident preparedness and operational continuity management*
- [RD 19] NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010

- [RD 20] “*Easy Access Rules*”, EASA eRules. Available at: <https://www.easa.europa.eu/document-library/easy-access-rules?page=3>
- [RD 21] “*Easy Access Rules for Air Traffic Management / Air Navigation Services*”, EASA eRules. Available at: [https://www.easa.europa.eu/sites/default/files/dfu/Easy\\_Access\\_Rules\\_for\\_ATM-ANS.pdf](https://www.easa.europa.eu/sites/default/files/dfu/Easy_Access_Rules_for_ATM-ANS.pdf)
- [RD 22] Regulation (EU) 2016/679, *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, 27<sup>th</sup> April 2016
- [RD 23] Directive (EC) 2008/114, *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, 8<sup>th</sup> December 2008
- [RD 24] “*Air Traffic Management Security Policy*”, NATO/EUROCONTROL ATM Security Coordination Group, 5<sup>th</sup> October 2015
- [RD 25] ICAO Doc. 10108 (Restricted), *Aviation Security Global Risk Context Statement*, 1<sup>st</sup> Edition, 2017
- [RD 26] ECAC Doc. 30 Part II (Restricted), *Security*
- [RD 27] EUROCAE ED205A, “*Process Standard for Security Certification and Declaration of ATM/ANS Ground Systems*”, 18<sup>th</sup> July, 2022
- [RD 28] “*CANSO Standard of Excellence in Cybersecurity*”, CANSO Cyber Safety Task Force, September 2020.
- [RD 29] “*Strategy for Cybersecurity in Aviation*”, EASA European Strategic Coordination Platform, 10<sup>th</sup> September 2019
- [RD 30] Regulation (EU) 72/2010, *laying down procedures for conducting Commission inspections in the field of aviation security*, 26<sup>th</sup> January 2010
- [RD 31] ISO/IEC 27005:2018 *Information technology – Security techniques – Information security risk management*
- [RD 32] ISO/IEC 31000:2018 *Risk management – Guidelines*
- [RD 33] ISO/IEC 27002:2013 *Information technology – Security techniques – Code of Practice for information security controls*
- [RD 34] Académie de L’air et de L’espace, Dossier #45, *Cyberthreats Targeting Air Transport*, January 2019



## 2. ATM Security Oversight

### 2.1 Overview

ATM Security is described by ICAO ([RD 5] 3.7) as follows:

*“The contribution of the ATM system to civil aviation security, national security and defence, and law enforcement; and the safeguarding of the ATM system from security threats and vulnerabilities.”*

Consequently, ATM security has the following dual requirements ([RD 5] 3.8):

- protection of the ATM system against threats and vulnerabilities;
- the provision of ATM security services in support of organisations and authorities engaged in aviation security, national security, defence, and law enforcement.

Thus, the ATM security role has a traditional internal role of protection of the ATM system itself, and an operational role in the support of certain aspects of aviation security as well as national security and law enforcement.

An additional guiding principle for ATM system operation and maintenance is to ensure the continuity of the ATM service against a variety of threats ([RD 5] 4.5):

*“The realization of this concept [continuity of service] requires contingency measures to provide maximum continuity of service in the face of major outages, natural disasters, civil unrest, security threats or other unusual circumstances.”*

Consequently, when system protections fail, service degradation should be limited, and service provision should recover in an orderly and timely manner, making the system resilient to attack through the implementation of contingency plans ([RD 5] 6).

Security oversight is a compliance monitoring and verification process by which security authorities obtain evidence that the required and expected security performance is met by stakeholders in the ATM/ANS system.

Oversight is addressed by regulations and guidance material produced by ICAO for Member States globally, and also by regional (the European region is addressed herein) and national bodies.

### 2.2 Applicable Rules and Regulations

Figure 1 depicts regulations and guidance material relevant to aviation security. Brief summaries of the regulations addressed in the following paragraphs are provided in ANNEX D – Document Summaries, along with a brief description of the applicability of each.

#### 2.2.1 Global

ICAO has identified and defined eight Critical Elements (CE) which are required for the effective implementation of security-related policies and associated procedures. A State's capability for security oversight is indicated by the status of implementation of the CEs, which are as follows:

	<b>Critical Element</b>
CE-1	Primary Aviation Security Legislation
CE-2	Aviation Security Programmes and Regulations
CE-3	State Appropriate Authority for Aviation Security and its Responsibilities
CE-4	Personnel Qualifications and Training
CE-5	Provision of Technical Guidance, Tools and Security-Critical Information
CE-6	Certification and Approval Obligations
CE-7	Quality Control Obligations
CE-8	Resolution of Security Concerns

**Table 1 – Critical Elements for Security Oversight**

These CEs are defined in ICAO Doc. 10047 [RD 6], which is directed at high-level government decision makers. It outlines the duties and responsibilities of ICAO Member States with respect to the establishment and management of a national civil aviation security oversight system. The CEs are required for the establishment, implementation, and maintenance of a State's civil aviation security oversight system, and supports the foundation of such a system. In Europe, EASA verifies through its standardised inspections that the states have implemented the CEs.

The following ICAO publications address the implementation and governance of aviation and ATM security:

- ICAO Annex 17, Safeguarding International Civil Aviation Against Acts of Unlawful Interference [RD 2]
- ICAO Doc 8973, Aviation Security Manual [RD 3]
- ICAO Doc 9807, USAP CMA [RD 4]
- ICAO Doc 9985, ATM Security Manual [RD 5]
- ICAO Doc 10047, Aviation Security Oversight Manual [RD 6]
- ICAO Doc 10108, Aviation Security Global Risk Context Statement [RD 25]

ICAO Member States are required to comply with the ICAO Annex 17 SARPs [RD 2].

ICAO Doc. 10047 [RD 6], together with ICAO Doc. 8973 [RD 3], provides guidance on how States can comply with the various SARPs of Annex 17 [RD 2]. They also describe the requirements and guidelines for the establishment and management of an effective aviation security and oversight system.

### **NCASP**

A State's aviation security policy and associated regulations, standards, measures, practices, and procedures should be reflected in the National Civil Aviation Security programme (NCASP).

For the purposes of this document, 'entity' refers to any public or private organisation involved in implementing aviation security measures, and subject to quality control activities. Each entity in a State should be consistent with the NCASP, which is described in detail in Chapter 6 of ICAO Doc 8973 [RD 3]. An NCASP model is provided in Appendix 1 of Doc 8973.

A major component of an NCASP and the main responsibility of the appropriate authority is aviation security oversight. In the context of the NCASP, security oversight encompasses the national obligations to:

- establish and properly staff a security organisation; develop laws, regulations, programmes, policies and procedures; and
- ensure that these requirements are effective, are being implemented, and are sustainable.

States should also develop and implement a comprehensive National Civil Aviation Security Training Programme (NCASTP) to ensure that function-specific training is provided to all persons involved in or responsible for the implementation of the NCASP. Each entity in a State should ensure that all personnel are appropriately trained and, where necessary, certified to perform their function, and be consistent with the NCASTP.

### **NCASQCP**

The National Civil Aviation Security Quality Control Programme (NCASQCP – often represented as NQCP) should be developed and maintained in cooperation with all entities involved in implementing aviation security measures, and the programme should be explained to any entity that could be subject to quality control activities.

Guidance on the NCASQCP is described in detail in Chapter 7 of ICAO Doc 8973 [RD 3]. The objective of the NCASQCP is to ensure the effectiveness of State regulations and the NCASP.

ICAO Doc. 8973 includes an index indicating where guidance material is provided for each SARP. While the methods of compliance provided there are based on generally recognized practices and procedures which are common within the international civil aviation industry, they are not the only means of compliance, and other methods of meeting the SARPs may be equally appropriate. Guidance material which is specific to ATM is provided in ICAO Doc. 9985 [RD 5].

### **USAP-CMA**

The Universal Security Audit Programme Continuous Monitoring Approach (USAP-CMA) also uses the CEs to assess a State's capability in security oversight.

The NCASP implementation will be monitored under the USAP-CMA framework and verified during USAP-CMA activities, which are described in ICAO Doc. 9807 [RD 4].

## **2.2.2 The European Region**

The following EU Regulations and Directives are applicable:

- Regulation (EU) 2017/373, Common requirements for providers of ATM/ANS services [RD 8] amended by Regulation (EU) 2020/469 [RD 9]
- Directive (EU) 2016/1148, Network and Information Security [RD 15]
- Regulation (EU) 2018/1139, New EASA Basic Regulation [RD 12]
- Regulation (EU) 2019/881, Cybersecurity Act [RD 13]
- Regulation (EU) 2015/1998, Detailed measures on aviation security [RD 11], amended by Regulation (EU) 2019/1583 regarding cybersecurity measures [RD 16]

Within Europe, in order to promote a harmonised approach to meeting Annex 17 SARPs, the current ATM-specific Implementing Regulation (IR) applicable to ATM Security is Regulation (EU) 2017/373 [RD 8] and its amendments (such as Regulation (EU) 2020/469 [RD 9]), which specify security requirements for ANSPs (including Flow Management functions) and the EUROCONTROL Network Manager (NM).

Consequently, Regulation (EU) 2017/373 [RD 8] and its amendments are the primary focus of this document.

Figure 1 shows the regulations and guidance material relevant to aviation security at the European Level. Regulation (EU) 2017/373 [RD 8] applies to ANSPs and to the EUROCONTROL NM, each of which are subject to oversight by NSAs, and may also be subject to oversight by EASA. Since EUROCONTROL Network Management facilities are situated in Belgium and France, they are also subject to the national security regulations of those countries.

EUROCONTROL also provides Guidance Material for EUROCONTROL Member States and contributes to Guidance Material and standards development in a number of forums.

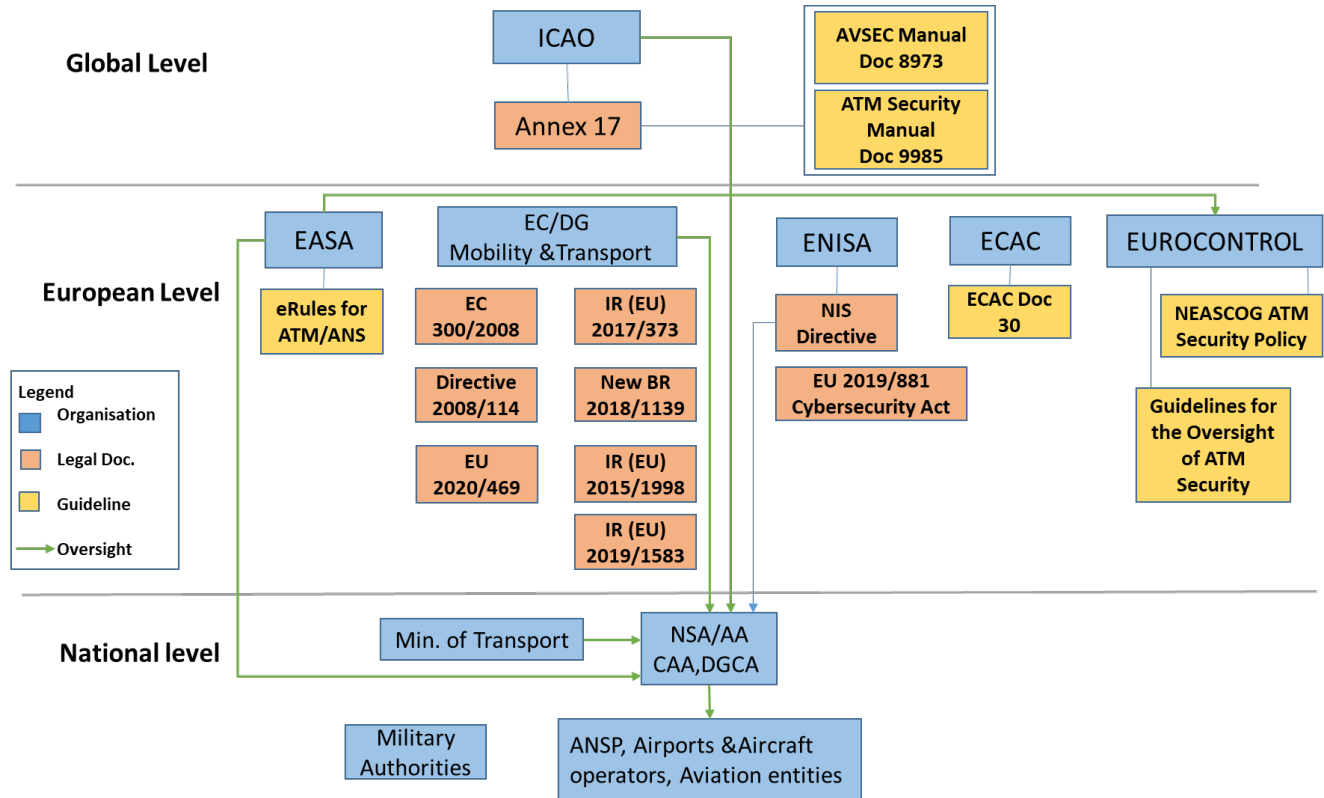


Figure 1 – Regulations and Guidance Material

### 2.2.3 Regulatory Complexity

In addition to complying with aviation-specific European regulations, operators may also have to comply with other legal instruments that apply to industry in general, such as the General Data Protection Regulation (GDPR) [RD 22], the Network and Information Security (NIS) Directive [RD 15], and the Cybersecurity Act [RD 13], which can make the task of maintaining regulatory compliance rather complex. If an operator happens to be designated as part of ‘critical infrastructure’ or as a ‘provider of an essential service’, it may also become subject to additional regulations and be required to report to additional authorities.

For example, the EU Common Requirements Regulation [RD 8] lays down security requirements to be followed by ANSPs, with audits being carried out by the National Supervisory Authority (NSA) or the European Union Aviation Safety Agency (EASA). However, if an ANSP is also designated as a provider of an essential service, it must comply with the NIS Directive [RD 15] and coordinate with the National Competent Authority (NCA) and/or the Computer Security Incident Response Team (CSIRT) for the notification of incidents having a significant impact on service provision. It must also comply with the Cybersecurity Act [RD 13], so its products, services, and processes are subject to the European Cybersecurity certification framework via ENISA.

This results in a more complex governance framework for providers of essential services, requiring the creation of additional roles and bodies, and resulting in additional coordination both within and outside member states.

## 2.2.4 Harmonisation

The need for rationalising and harmonising the complex regulatory framework for aviation in Europe resulted in EASA creating the European Strategic Coordination Platform (ESCP) with stakeholders from all aviation domains, to address cybersecurity strategy, risk assessment methods, the sharing of risk information between organisations, and to address gaps and overlaps in the regulatory framework. The ESCP has developed a Strategy for Cybersecurity in Aviation [RD 29] to make aviation an evolutionary cyber-resilient system, adopting a 'built-in' security approach and addressing security from a system's conception through its development, deployment, and operations.

In support of this development, in 2019, EASA created 'Rulemaking Task' (RMT) RMT.0720, which proposed to introduce provisions for the management of cybersecurity risks by organisations in all aviation domains (design, production, continuing airworthiness management, maintenance, operations, aircrew, aerodromes, and ATM/ANS). These provisions would include high-level performance-based requirements, and would be supported by Acceptable Means of Compliance (AMC), Guidance Material (GM) and industry standards. A proposal was provided to the European Commission in 2021, and adoption is expected in late 2022.

## 2.3 Assumptions

In this document, it is assumed that, in accordance with ICAO Annex 17 [RD 2], the NCASP has been developed, implemented, and is being maintained in cooperation with applicable entities within a State, and that its quality is being monitored as part of the NCASQCP.

ICAO Annex 17 specifically refers to air traffic service providers in Standard 3.5, which states:

*"Each Contracting State shall require air traffic service providers operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State."*

The specific interpretation of this Standard and the manner in which the provisions are implemented are, however, at the discretion of the participating State. In order to ensure a harmonised approach to certification and oversight among EU Member States, Regulation (EU) 2017/373 [RD 8] (and its amendments) are currently in place to facilitate the implementation of a harmonised approach across EU Member States.

In common with other regulations, it provides several numbered introductory statements prior to Article 1 (known as 'recitals') which set out concise reasons for the main provisions of the enacting terms. For example: recital (4) refers to common rules for the certification and oversight of service providers; recital (5) refers to the coordination of measures to be implemented for the security of systems, constituents in use and data; recital (6) refers to security vulnerabilities which have an impact on safety. It also recommends that the NSA should be independent from the service provider (recital (9)), and that technical personnel involved should be subject to a harmonised training and competence assessment scheme (recital (12)).

The assumption of this document is that Member States have put a number of arrangements in place but require guidance on the implementation of an oversight process focusing on ATM security.

## 3. Guidance for ATM Security Oversight

### 3.1 The Oversight Programme

The ATM Security Oversight Programme is an integral part of the overall National Aviation Security (AVSEC) Programme (through the National Quality Control Programme). Security oversight is a joint activity involving the Competent Authority (CA), the Audit Team, and the Entity.

These guidelines recommend that a single CA should be responsible for the National ATM Security Oversight Programme, however a State may nominate or establish more than one CA under certain conditions (see [RD 8] Article 4.4). To ensure impartiality and transparency when exercising their powers, CAs must be independent of the Entity concerned (see [RD 8] Article 4.5). These guidelines recommend that roles or links with other authorities responsible for security, such as the CAA, AA, or NCA, should be clarified.

These guidelines recommend that the CA establishes, and updates annually, an oversight programme taking into account the specific nature of the service provider, the complexity of their activities, and the results of past certification and/or oversight activities, based on the assessment of associated risks.

#### 3.1.1 ICAO Security Monitoring Activities

Security monitoring activities of the following types are described in ICAO Doc. 8973 ([RD 3] 7.4.2), and further details are provided in ANNEX B – Security Monitoring.

- **Audit:** An in-depth compliance examination of all aspects of the national civil aviation security programme implementation.
- **Inspection:** This examines the implementation of relevant national civil aviation security programme requirements by an ANSP.
- **Test:** A security test is a simulation of an attempt to commit an unlawful act that tests an aviation security measure. A security test may be overt or covert.
- **Survey:** An evaluation of security needs including the identification of vulnerabilities which could be exploited to carry out an act of unlawful interference, and the recommendation of corrective actions.

If the approach of ICAO Doc. 8973 is followed by an Entity, the results of security monitoring activities may be documented in terms of the compliance classification scheme described within it ([RD 3] 7.4.4; see Annex C.1). Such information may be used by an Entity to prioritise corrective actions to address security deficiencies, and it may also be provided as one of the inputs to the oversight activities described by Regulation (EU) 2017/373 [RD 8].

The resources required of oversight actors, and the duration of their activities, depend on the type of oversight task being carried out. The skills required by Audit Team members with respect to security requirements are described in ANNEX E – Applicable Requirements and Audit Team Skills.

#### 3.1.2 SES ATM Security Regulatory Requirements

An indication of the scope of oversight activities which must be carried out is provided by the security requirements of Regulation (EU) 2017/373 [RD 8] and its amendments.

The focus of Regulation (EU) 2017/373 is on preventing unlawful interference in the provision of services. This is addressed by specifying security requirements in areas which include security management systems, contingency plans, personnel requirements, and staff training.

Security non-conformities which may have an impact on safety are an additional concern during the oversight process. To ensure that these are identified and addressed, all security non-conformities should be shared with Audit Team members who are familiar with safety requirements. This is briefly addressed in section 4.5.

The following sections describe the main security requirements within this regulation, as well as some which have an overlap with safety.

Oversight of compliance with safety requirements may be the responsibility of members of the audit team not directly involved in security oversight, but it is important to be aware of potential interdependencies.

### 3.1.2.1 ATM/ANS.OR.D.010 Security Management

This section of the Regulation contains the primary security management requirements, which are depicted in Figure 2, and are presented in Annex E.2, Table 17 along with corresponding audit team skill requirements.

A Service Provider must establish a Security Management System (SeMS) to protect facilities, personnel, service provision and operational data. The SeMS must also define procedures relating to security risk assessment, risk mitigation, security monitoring, security improvement, security reviews and lesson dissemination.

Incident management is also in scope, with requirements to detect security breaches and alert personnel. Resilience is also addressed, since the means of containing breaches must be established, along with capabilities to identify recovery and mitigation actions.

An Entity must also ensure that personnel have appropriate security clearance, which may require different levels of clearance depending on roles.

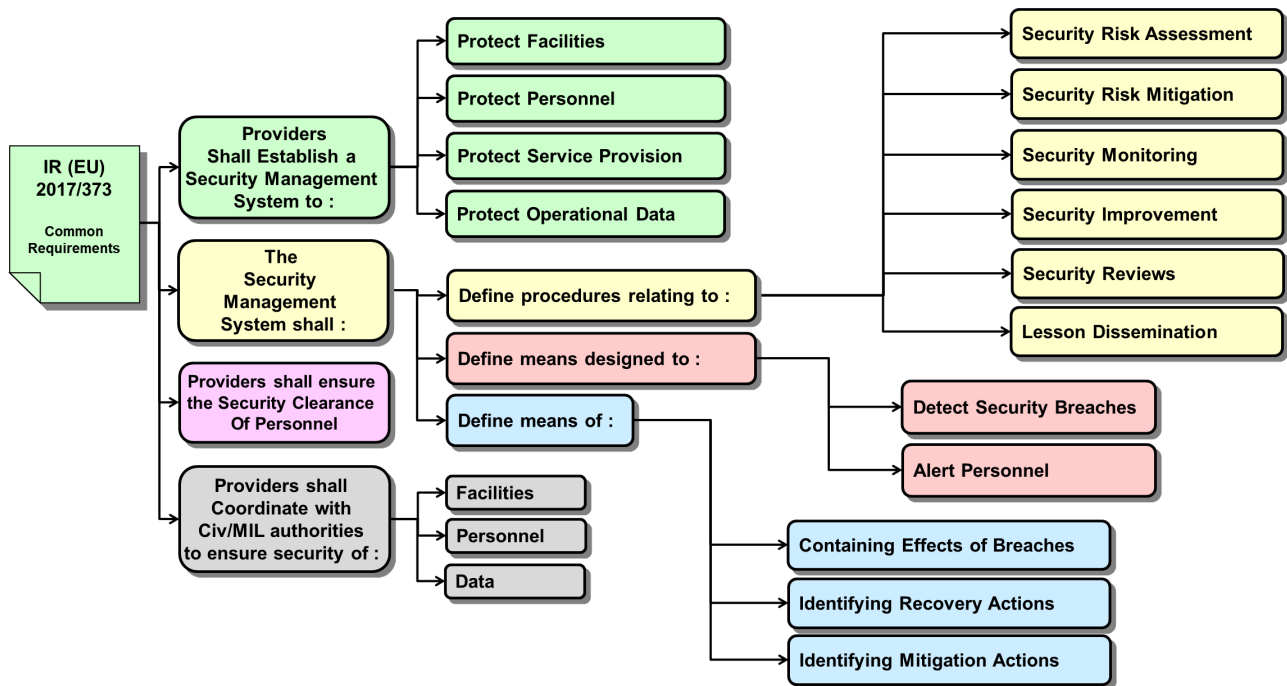


Figure 2 – Security Requirements from Regulation (EU) 2017/373

### 3.1.2.2 ATM/ANS.OR.B.005 Management system

This section of the Regulation specifies a number of general management system requirements (Annex E.1, Table 16) which are applicable to an organisation. These requirements are not specific to security management, but compliance with them is a necessary pre-requisite for requirements described in 3.1.2.1 to be met. The requirements include:

- Clearly defined lines of responsibility and accountability



- A policy on safety, quality, and security of services
- Performance indicators to assess actual performance against targets
- A process to ensure that personnel are trained and competent to perform their duties in a safe, efficient, continuous and sustainable manner
- Policies for the recruitment and training of personnel
- A compliance monitoring function

### 3.1.2.3 ATM/ANS.OR.A.070 Contingency Plans

If a security incident results in significant degradation or interruption of service provision, contingency plans must be in place to support recovery to normal operations. This requirement is described in the Contingency Plans section of the Regulation in Annex E.4, Table 19, along with audit team skill requirements with respect to security.

### 3.1.2.4 ATM/ANS.OR.B.020 Personnel requirements

This section of the Regulation specifies requirements on the accountability and authority of managers, and the duties and responsibilities of personnel, including those in security:

- Accountable management responsible for establishing and maintaining an effective management system and ensuring that activities are appropriately financed
- Definitions of the authority, duties, and responsibilities of post holders (including those in security)

The requirements are presented in Annex E.3, Table 18, along with audit team skill requirements with respect to security.

### 3.1.2.5 ATSEP.OR.105 Training and competence assessment programme

It is necessary that Air Traffic Safety and Electronics Personnel (ATSEP) are provided with appropriate specialist security training providing them with the competences to maintain the resilience of their systems. This requirement is described in Annex E.5, Table 20, and also applies to contracted ATSEP staff.

## 3.2 Recommended Oversight Process

Figure 4 depicts the oversight process as a Turtle diagram, showing a high-level view of the components which interact during the process, revealing inputs, outputs, actors, and other dependencies, which are now described in more detail.

## 3.3 Actors

The main actors in the oversight process are the Competent Authority (CA), the Audit Team, and the Service Provider. Depending on the approach taken by an individual Member State in the allocation of responsibilities to organisations, the Audit Team may reside within the CA, or it may reside in another organisation. In the example process described here, it is assumed that the Audit Team is incorporated within the CA.

The roles and responsibilities of the actors are now described.

### 3.3.1 Competent Authority

It is assumed that the State has developed an aviation security policy and associated regulations, standards, measures, practices and procedures, which is reflected in the National Civil Aviation Security Programme (NCASP) (a model is available in Doc 8973/9 Appendix 1[RD 3]). Each Entity in the State should be consistent with the NCASP.



The National Civil Aviation Security Committee (NCASC) promotes the coordination and consistency of policy implementation and standards at the national level.

The State will also have developed a National Civil Aviation Security Training Programme (NCASTP), which ensures that appropriate training is provided to all persons involved in, or responsible for, the implementation of the NCASP. However, the need for additional guidance in the area of ATM Security oversight has been expressed.

The National Civil Aviation Security Quality Control Programme (NCASQCP / NQCP), ensures the effectiveness of the NCASP in each entity. ATM Security Oversight is a component of the NQCP. The N(CAS)QCP should be organised independently from the entities and persons responsible for implementing NCASP measures.

Within the State, it is the responsibility of the Competent Authority to carry out the oversight task. ICAO refers to the designated Appropriate Authority (ICAO Doc 8973 2.1.2, 5.1.1 [RD 3]), while ECAC Doc. 30 [RD 26] refers to the 'relevant authority'.

The SES Regulatory framework specifies that a National Supervisory Authority (NSA) (Regulation (EC) No 549/2004 [RD 7] Art. 4) is responsible for the oversight of the common requirements (including security requirements in Regulation (EU) 2017/373 [RD 8]). This document will henceforth refer to the body responsible for carrying out the oversight task as the Competent Authority (CA).

### **3.3.2 Audit Team**

These guidelines recommend that an Audit Team should be composed of the following members:

- A team leader
- One or more security inspectors
- One or more administrative assistants

Inspectors should be appropriately qualified and trained to address each of the security areas to be inspected. The requirements of Regulation (EU) 2017/373 [RD 8] (see ANNEX E – Applicable Requirements and Audit Team Skills), indicate that an oversight activity requires inspectors who are appropriately qualified and trained to address areas which include the following:

- Security management systems
- Security risk assessment
- The incident management process
- Facilities
- Personnel
- Cybersecurity of IT systems and interfaces
- Communications, Navigation, and Surveillance systems

The necessary skills must be acquired by audit team members via the established NCASTP, and trainees should pass a valid, standardised exam at the end of their training courses. This ensures that adequate standards are consistently achieved.

Quality control personnel should be independent from the entities being monitored, and the results of oversight activities should remain strictly confidential.

### **3.3.3 Service Provider**

As described in the previous section, the scope of an audit may require the input of a broad range of personnel within the Service Provider, possessing expertise in the areas being addressed by the planned oversight activity.

### 3.4 Systems and Tools

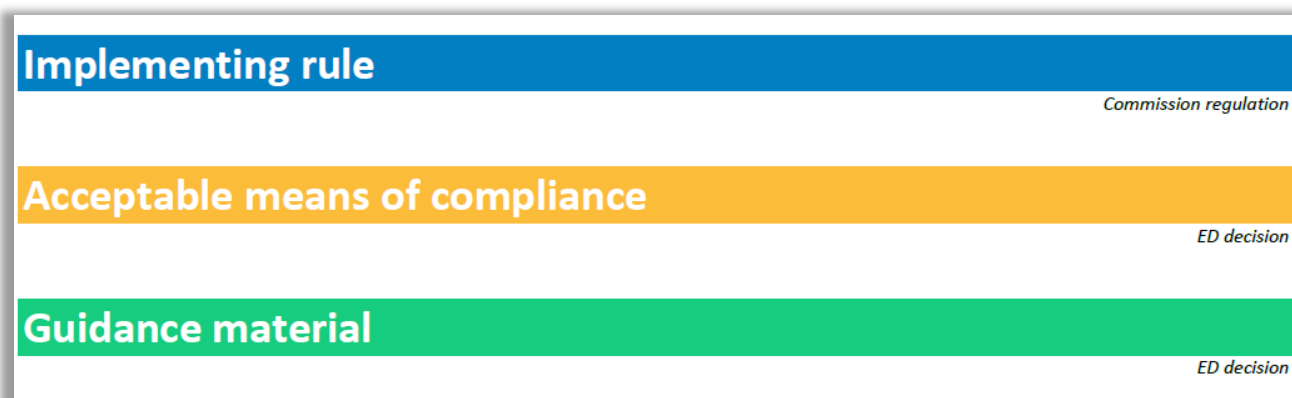
The CA, Audit Team, and Entity must be able to effectively communicate and create, modify, share, and provide feedback on documents which are developed during the oversight process. This requires the use of compatible tools (e.g. word processing, spreadsheet, database software) by all parties.

There are several circumstances where it may be beneficial to perform compliance monitoring activities remotely using email, and compatible tele- and/or video-conferencing applications. Such circumstances may include the following:

- Only brief, focused activities are required, which are easy to perform remotely
- An Entity may have reason to minimise the number of external visitors on-site
- A CA may have reason to minimise the external deployment of Audit Teams

It is necessary to ensure that the mechanisms used for remote oversight ensure compliance with regulations in the areas of personal privacy, data privacy, ensure the protection of sensitive information, and comply with all applicable laws. Due to the emergence of SARS-COV-2, and the possibility of similar situations occurring in the future, it may become more common to perform certain certification and regulatory oversight activities remotely.

A generally available tool that facilitates comprehension of the regulatory framework in Europe is the EASA eRules [RD 20] (also known as Easy Access Rules) a comprehensive system developed by EASA for the drafting, sharing and storing of rules.



**Figure 3 – EASA eRules Colour Coding**

It is a single source for all aviation safety rules applicable to European airspace users, offering easy (online) access to all rules and regulations as well as cross-referencing, and comparison with ICAO and the standards of third countries.

A colour code, as shown in Figure 3, is used to differentiate references to EU Implementing Rules, Acceptable Means of Compliance (AMC), and Guidance Material. The rules for ATM/ANS associated with Regulation (EU) 2017/373 [RD 8] and its amendments are explained by the EASA Easy Access eRules document [RD 21]. However, this is not an official publication and a disclaimer states that “EASA accepts no liability for damage of any kind resulting from the risks inherent in the use of this document”.

At the time of writing, there is little in the way of AMCs and Guidance Material available in the area of security, but this will change in the future.

### 3.5 Controls and Checks

The process described specifies start points and end points, and requires that certain intermediate deliverables are agreed by the Entity and the CA for the activities to progress.

EASA may perform standardisation inspections of National Supervisory Authorities, and may also perform oversight activities on Service Providers.

### 3.6 Risks

The following risks should be considered while planning and performing oversight activities:

- There is a shortage of experienced auditors in key areas, such as cyber-security
- The oversight activity requires significant time and effort from the Entity
- The oversight activity may impact normal operations and service provision

### 3.7 Opportunities

The oversight process may present opportunities, such as the following:

- Non-compliances are identified and rectifications are planned and implemented appropriately
- Minor non-compliances are prevented from accumulating or evolving into more serious issues
- Significant non-compliances are rectified urgently to rapidly mitigate potential risks
- Oversight activities promote compliance and reduce the likelihood of non-compliances, which may potentially result in legal and regulatory consequences

### 3.8 Performance Indicators

Performance indicators (PIs) should encompass information on security events associated with the broad variety of assets which are within scope. This includes information on events associated with physical infrastructure, information systems, social engineering (including insider events), organisational issues, and indicators on service provision.

PIs may include:

- Number of physical security breaches
- Number of unauthorised persons accessing restricted areas
- Instances of theft of equipment or information
- ...

In the area of cybersecurity, a number of useful indicators will be available from Security Operations Centres (SOCs), which may include the following:

- Number of malware events
- Number of phishing events
- Number of alerts, and number of positive alerts
- Alerts escalated
- Mean time to detect (MTTD), mean time to respond (MTTR)
- ...

More general PIs may include:

- Number of security policy violations

- Cost of incidents
- Number of risk assessments completed
- Number of security controls deployed
- ...

### 3.9 Inputs

The CA and the Entity agree on an Oversight Programme, to be reviewed annually. This describes the scope and schedule of oversight activities over a planning cycle of typically 24 months. The oversight planning cycle may be extended or reduced depending on the compliance performance of the Entity<sup>1</sup>.

### 3.10 Outputs

The final outputs of the process are the following:

- The Audit Report
- The Follow-up Audit Report
- The Closure Letter

Descriptions of these documents are provided in ANNEX F – Process Documents.

---

<sup>1</sup> [RD 7] ATM/ANS.AR.C.015 Oversight Programme (a) (5)

## 4. Process Steps

Oversight activities should be carried out in a standard systematic way to achieve consistency in the consolidation and comparison of Audit Findings and recommendations. In addition, the CA and Audit Team should ensure that oversight activities have no impact on normal operations.

The process described here is elaborated from that contained within Regulation (EU) No 628/2013 [RD 14], on working methods for conducting EASA standardisation inspections. This process addresses the elements recommended for consideration in the methodology described in the AVSEC manual ([RD 3] 7.4.2.7).

Note that some of the documents resulting from the implementation of this process may contain sensitive or restricted information. Consequently, they must be classified appropriately and disseminated only to those authorized to access them, in accordance with national rules for the protection of such information.

Individual process steps are depicted in Swim-lane diagrams in Figure 5 and Figure 6, and are now described in details.

### 4.1 Start Point

From Figure 5, the event that triggers the process may be one of the following:

- A planned activity in an existing audit schedule
- A follow-up to a previous audit is scheduled
- A decision is made by an authority to perform an ad-hoc oversight activity (e.g. due to the occurrence of a security incident)

### 4.2 Initiation

It is the responsibility of the CA to inform an Entity in writing that security oversight activities are to take place.

The CA, in cooperation with the Audit Team, will develop both the Expectations of the activity and a draft Programme. These documents may address findings from a previous audit which are still open.

Step	Description
Starting Point:	<ul style="list-style-type: none"> <li>- A regular audit is scheduled in the Annual Oversight Programme</li> <li>- A follow-up to a previous audit is scheduled</li> <li>- A decision is made by an authority to perform an ad-hoc oversight activity</li> </ul>
Step 1	The CA sends a letter to the Entity informing it of an upcoming oversight activity in line with national legislation and procedures, and summarising the legal basis
Step 2	The CA develops the Expectations document
Step 3	The CA develops the Draft Programme
Step 4	The Audit Team uses this information to select appropriately qualified and experienced individuals to participate in the activity.
Step 5	The documents described in Steps 1, 2, and 3 are reviewed by the CA, Audit Team, and Entity
Step 6	The documents reviewed in Step 5 are approved by correspondence, and if necessary by conference call or physical meeting
End Point:	Final versions of the Expectations and Oversight Programme documents are approved

**Table 2 – Initiation Steps**

The Oversight Programme describes the scope and the schedule of the upcoming activity.

With regard to the “Expectations” document and other elements to be checked during an audit, Table 23 in ANNEX H provides an example of how regulatory requirements and guidance material might be used in the development of check-lists for CAs. The suggested examples of “Expectations” shown in this table have been obtained from the Guidance Material referenced in ANNEX G, Table 22. CAs typically develop their own “Expectations”.

The additional columns in Table 23 include “Means of Compliance”, “Evidence Available / Supplied”, “Compliance Assessment Result”, and “Corrective Action Required”, and are simply suggestions based on the oversight process described in this document.

Table 23 could also be used as a basis for an Entity to develop a Self-Assessment questionnaire.

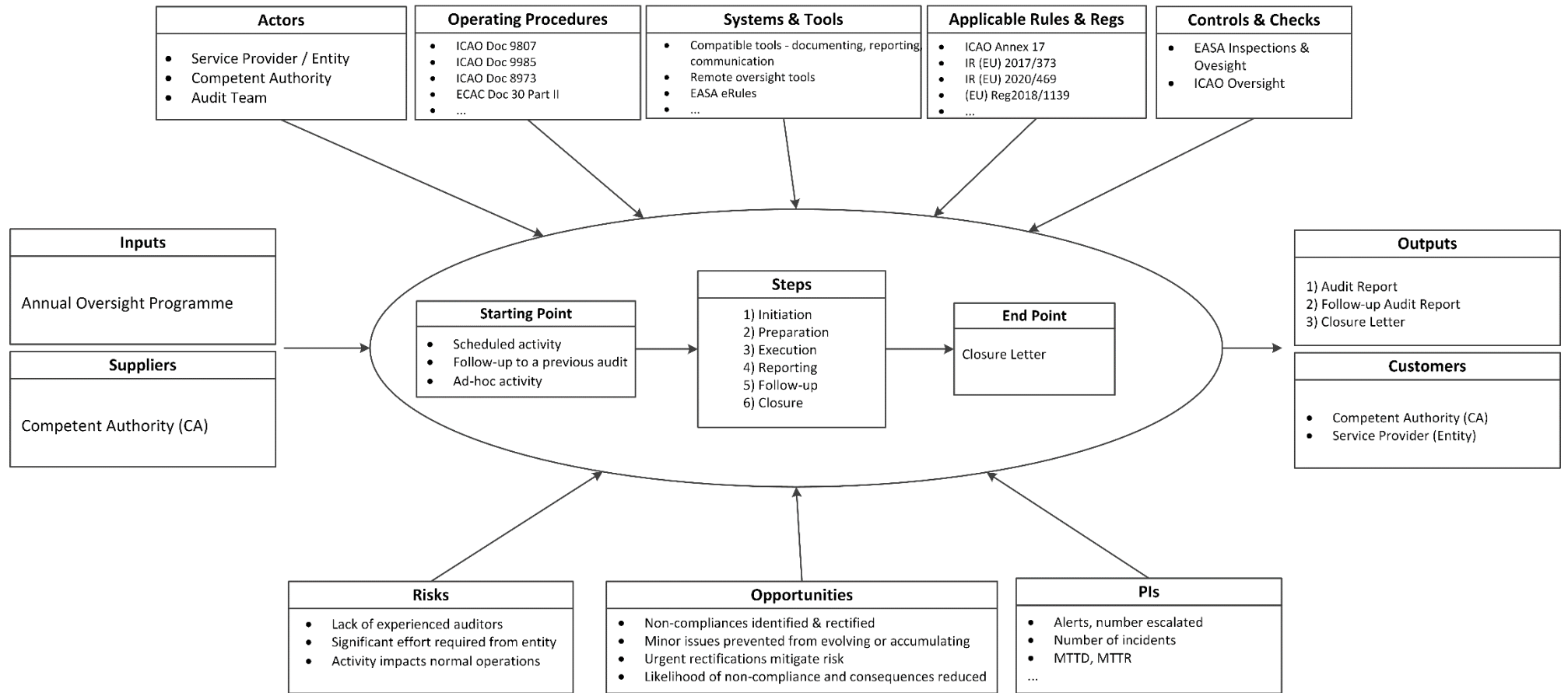


Figure 4 - Oversight Process Turtle Diagram

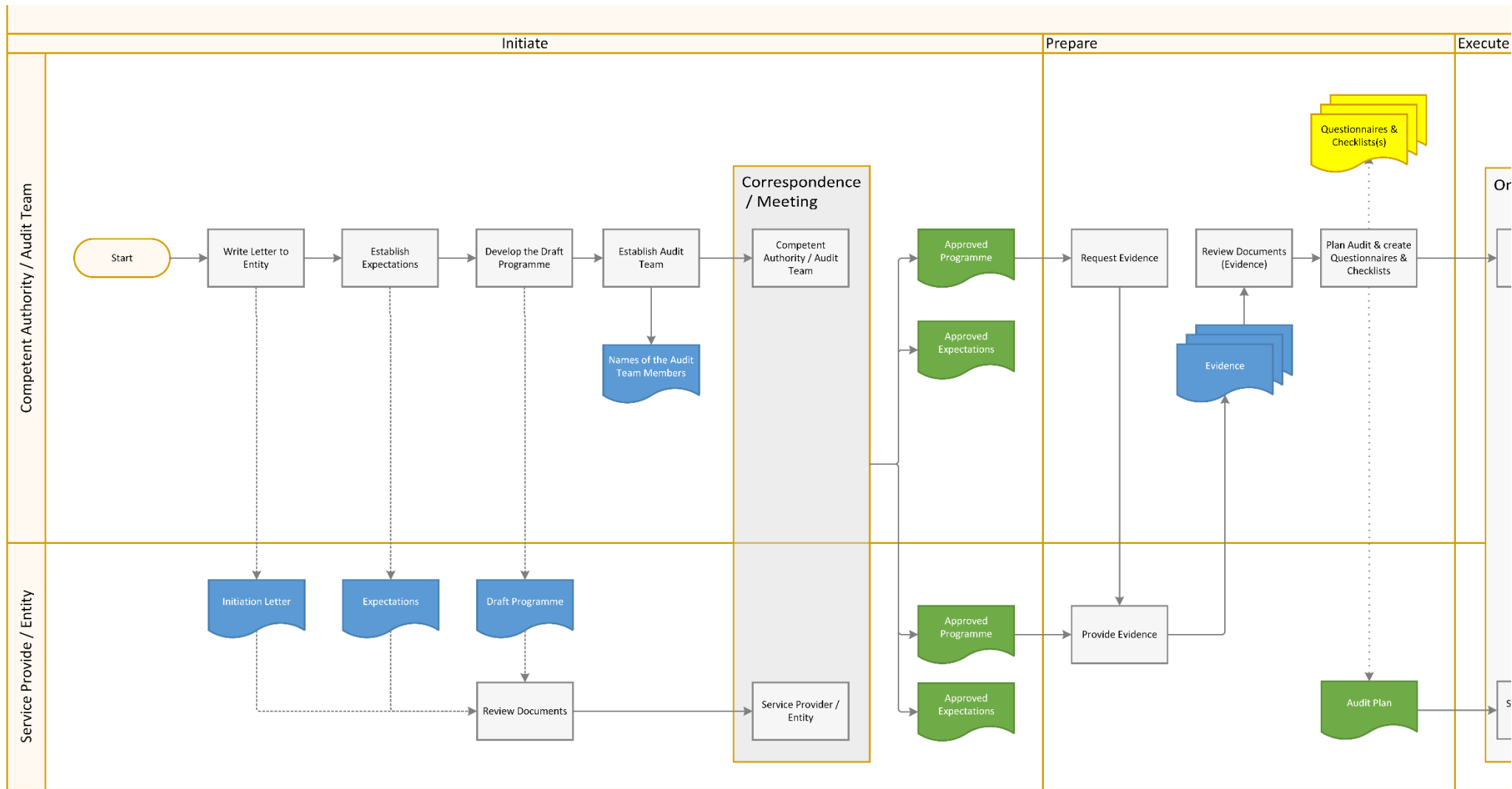


Figure 5 – Oversight Process (Part 1)



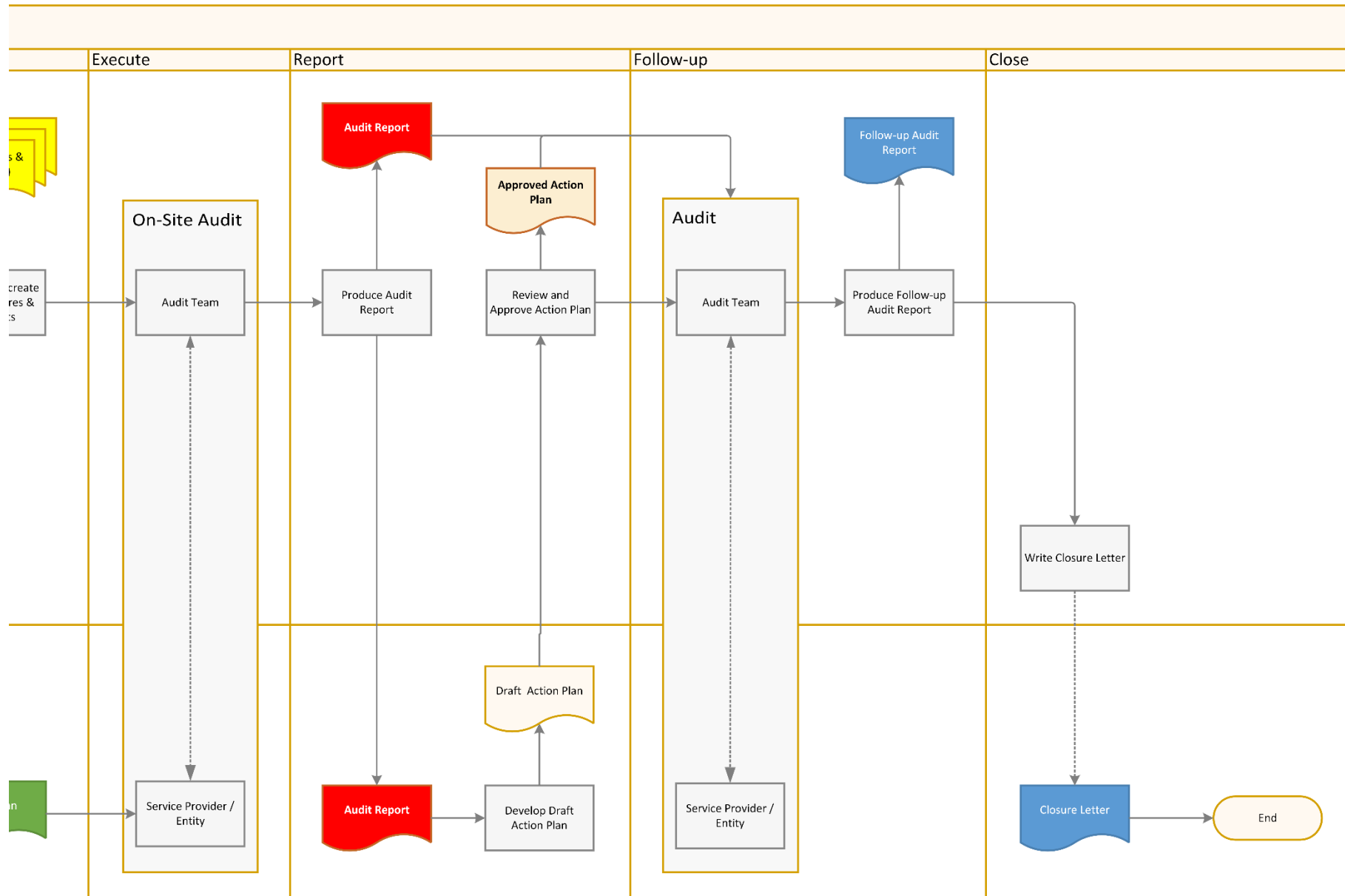


Figure 6 – Oversight Process (Part 2)

## 4.3 Preparation

For each oversight activity within the programme, several preparatory activities take place. These guidelines recommend that a preparatory phase begins a number of weeks prior to the on-site oversight activities. The duration of the preparatory phase depends on the particular CA. The appointed Audit Team Leader allocates team members by matching their skills and experience to specific oversight activities. Recommendations for Audit Team skill requirements are provided in Annex F.

Desktop activities typically performed during this phase include becoming familiar with the following aspects related to the Entity:

- The objective and scope of the oversight activity
- Entity points of contact
- Geographical deployment
- Asset inventory
- Initial or ongoing oversight activities
- Previous audit reports
- Ongoing compliance issues

Step	Description
Starting Point:	Programme and Expectations documents have been approved
Step 1	The Entity is contacted and requested to provide Evidence including means of compliance, in accordance with the contents of the Expectations and Programme documents.
Step 2	The Entity provides the requested Evidence to the Audit Team
Step 3	The Audit Team reviews the Evidence, comparing it with the requirements, and identifying priorities for oversight
Step 4	The Audit Team develops detailed Questionnaires and Checklists for use by the Audit Team during the oversight process. Questionnaires (or parts thereof) may optionally be shared with the Entity
Step 5	The Audit Team produces a detailed Audit Plan for the on-site audit, which includes a detailed schedule and the allocation of audit lots to each Audit Team member. The Audit Plan is agreed with the Entity.
End Point:	The Audit Plan is agreed with the Entity and approved

**Table 3 – Preparation Steps**

The audit is normally performed by the audit team. However, if there is a lack of resources to perform their tasks, they may invite other auditors to assist with the activities from a pool of European aviation inspectors (see New Basic regulation 2018/1139 (article 63) [RD 12]).

In other cases, the CA may delegate the responsibility for carrying out audit activities to a qualified entity. The responsibility for certification of the Entity remains with the CA or EASA.

## 4.4 Execution

The execution phase is carried out on-site at the Entity, following the agreed Oversight Programme and the detailed Audit Plan, and using Questionnaires and Checklists developed during the Preparation phase.

Table 23 in ANNEX H provides an example of how regulatory requirements and guidance material might be used in the development of check-lists for CAs for use during the Execution phase of the oversight process.

Step	Description
Starting Point:	The Audit Plan is approved and all Questionnaires and Checklists have been completed
Step 1	The on-site oversight activity is carried out according to the Audit Plan. Activities carried out include: The Audit Team conducts interviews with personnel of the Entity having security roles and responsibilities. The Questionnaires and Checklists developed during the Preparation phase are used by the Audit Team to guide the activities.
End Point:	The on-site activities in the Audit Plan are completed

**Table 4 – Execution Steps**

The audit team may follow-up other issues as required.

## 4.5 Reporting

The Audit Team produces an Audit Report containing the Findings of the audit after the completion of the Execution phase. The timeframe depends on the particular CA.

The focus of Regulation (EU) 2017/373 [RD 8] is on preventing unlawful interference in the provision of services, however, it also addresses the oversight of areas of potential safety concern<sup>2</sup>, namely security non-compliances which have an impact on safety.

For the area of aviation security, specific compliance classification schemes exist. For example, the scheme described in the ICAO AVSEC manual [RD 3] has 5 levels of Audit Findings (See Annex C.1). In addition, Regulation (EC) 72/2010 [RD 30] describes a classification scheme for use in commission inspections in relation to Regulation (EC) 300/2008 [RD 10] which consists of 6 levels (see Annex C.2), and is very close to the AVSEC manual scheme (Annex C.1). An example of a possible mapping between these schemes is shown in Annex C.3. Use of these schemes for security compliance classification would provide a level of compatibility with both the ICAO and EC approaches.

The Evidence provided to the Audit Team during the Preparation phase and the information obtained during the Execution phase will be in a variety of forms, which may include documentation such as security risk assessments, completed questionnaires, and transcripts of interviews, from which may be extracted security non-compliances. For the purpose of reporting, it is necessary to translate information on security non-compliances into Audit Findings which reflect their potential impact on safety. An Audit Finding is a non-conformity in regulatory compliance with one or more aspects of EASA regulatory requirements, and they are classified according to their level of significance.

<sup>2</sup> ATM/ANS.AR.C.015 Oversight programme (a) (1) cover all the areas of potential safety concern ...

<b>Audit Finding</b>	<b>Description</b>	<b>Resolution time</b>
<b>Level 1</b>	Significant non-compliance	Immediate
<b>Level 2</b>	Non-compliance	Up to 3 months
<b>Observation</b>	Potential problem that could lead to non-compliance	Not applicable

**Table 5 – Regulation (EU) 2017/373 Compliance Classification Scheme**

Use of the compliance classification scheme in Regulation (EU) 2017/373 [RD 8] section ATM/ANS.AR.C.050 (also known as the EASA scheme) is widespread in the European region, independent of whether or not the State is subject to EU regulation. This scheme has 3 levels, as shown in Table 5, and they are described in more detail in Annex C.4.

Consequently, these guidelines recommend that all security non-compliances should be identified and examined to establish their potential impact on service provision and on safety, and reported in accordance with the scheme in Table 5.

To ensure that security non-conformities with a potential safety impact are identified, all security non-conformities should be shared for assessment with Audit Team members who are familiar with safety requirements.

Reporting phase steps are described in Table 6.

<b>Step</b>	<b>Description</b>
Starting Point:	The on-site activities in the Audit Plan are completed
Step 1	The Audit Team / CA drafts the Audit Report
Step 2	The Audit Report is shared with the Entity for review and approval
Step 3	The Audit Team / CA formally shares the approved Audit Report with the Entity
Step 4	The Entity produces a draft Action Plan to address the findings of the Audit Report, and provides this to the Audit Team and CA for review and approval
End Point	The Approved Action Plan is formally accepted by the Audit Team / CA.

**Table 6 – Reporting Steps**

The Audit Report addresses all aspects of the oversight exercise, and includes the following:

- documentation of the Audit Findings
- an assessment of compliance with the requirements of the NCASP
- corrective actions which are required, each with a proposed completion date

In response to the Audit Report, the Entity must propose a corrective Action Plan, to be submitted to the Audit Team Leader for approval. The Action Plan must address all Audit Findings and identify the following:

- a proposed corrective action for each Audit Finding, which must address the root cause of the Audit Finding
- a proposed completion date
- high priority corrective actions should be identified for completion as soon as is feasible

The Audit Report aims to record all Oversight Activities carried out, and may include the following information:

- dates and locations of the oversight activities
- the identification of the Entity
- the composition of the Audit Team
- identification of personnel interviewed
- the objectives and scope of the audit
- the audit schedule
- Audit Findings and observations on compliance

Documents used for compliance evaluation, such as those reviewed during the audit, are logged and kept under configuration management, but they are generally not included in the Audit Report.

These guidelines recommend that the Audit Report and the Action Plan are agreed between the Audit Team and the Entity before they are provided to the CA.

The following may be included as attachments to the Audit Report:

- Checklists and Questionnaires used by the Audit Team
- Evidence provided by the Entity (permission of the Entity required)

The Audit Report must be classified in accordance with national rules for the protection of sensitive information.

## 4.6 Follow-Up

The Follow-up audit is a formal activity conducted to:

- Monitor the implementation of the corrective action plan in coordination with the entity.
- Verify the implementation of corrective actions resulting from previous audits. This should be done after receiving details of the Action Plan, containing corrective actions and associated completion dates.
- Verification and closing-out of corrective actions

These guidelines recommend that the Audit Team creates the Follow-up Audit Report in coordination with the Entity before providing it to the CA.

However, a continuous oversight approach, where periodical Follow-Up reporting is carried out, is often considered to be better practice.

Step	Description
Starting Point:	The Audit Report and Action Plan are completed
Step 1	The Audit Team assesses the Entity on the implementation status of corrective actions with reference to the Action Plan
Step 2	The Audit Team verifies the completion of the implementation of the corrective actions
Step 3	Completed corrective actions are closed-out and recorded as such
Step 4	The Audit Team creates the Follow-up Audit Report in coordination with the Entity
End Point:	The Follow-up Audit Report is formally delivered to the CA

**Table 7 – Follow-up Steps**

## 4.7 Closure

Closure is the final phase of the oversight process.

After the CA has received the Follow-up Audit Report, the CA decides whether or not it is satisfied that the root causes of non-conformities have been addressed.

If that is the case, these guidelines recommend that the audit documents are signed-off, filed, and that a letter is sent to the entity informing it of the closure of the oversight activity.

The date of the Follow-up Audit and the verification actions are recorded. To avoid the possibility that similar Audit Findings are raised during subsequent oversight activities, these guidelines recommend that CAs should not keep non-conformities 'open' for extended periods of time.

Step	Description
Starting Point:	The Follow-up Audit Report has been completed and formally delivered to the CA.
Step 1	The CA assesses the Follow-up Audit Report to confirm that the root-causes of non-conformities have been adequately addressed.
Step 2	The audit documents are signed-off and filed.
End Point:	The Entity is informed formally by letter of the Closure of the oversight activity.

**Table 8 – Closure Steps**

## 4.8 End Point

The process is ended by the delivery of a formal letter to the Entity informing it of the Closure of the oversight activity.

## 5. Conclusions

This document presents a summary of applicable global and European rules and regulations for the security oversight of air navigation service providers.

The types of activities carried out in a typical oversight programme are described, and an oversight process is presented, which includes descriptions of the activities to be performed at each stage, and of the input and output documents required. The example process is intended to be illustrative, and would require to be adapted depending on the specifics of the CA and the Service Provider.

The supporting Annexes provide background material which includes information on security monitoring, EU and ICAO compliance classification schemes, and brief descriptions of referenced regulations and guidance material. Tables of applicable requirements for ANSPs are presented, along with descriptions of the skills required within an Audit Team to effectively perform oversight tasks.

Mappings of certain regulatory requirements to relevant guidance material in ECAC, ICAO, and CANSO guidance documents are also provided. These may be of use to ANSPs to assist them in compliance activities. They may also be of use to Auditors performing security oversight tasks.

Finally, an example of a check-list based on regulatory requirements is provided. Such information might be adapted by ANSPs for the purpose of self-assessment, and by Auditors for the purpose of producing questionnaires and check-lists for audit purposes.

## ANNEX A – Document Update Procedures

It is necessary to periodically check these EUROCONTROL Guidelines for consistency with referenced material, notably ICAO SARPS and relevant Regulations. The Guidelines may also evolve following feedback from field experience.

The main objectives of a regular review are:

- a) to improve the quality of the Guidelines (e.g. clarity, testability, etc.);
- b) to verify that the level of detail published is adequate;
- c) to make all stakeholders aware of the latest developments.

The update process for the guidelines is expected to be initiated by Stakeholders, who may provide change proposals either through existing working arrangements (e.g. established working groups) or by sending a formal Change Request (CR) to the generic email address: [standardisation@eurocontrol.int](mailto:standardisation@eurocontrol.int).

The CR needs to provide, at a minimum, the following elements:

- Originator information (name, organisation, contact details);
- Guideline title, number and edition date;
- Page, chapter, section (subsection) where the issue appears;
- Description of the issue and reason for change;
- Specific change proposal text (incl. potential alternatives, if any).

Main steps towards a revised version:

- EUROCONTROL will assess each CR in coordination with content owners to establish the urgency and impact (major, minor or editorial);
- A resolution proposal will be prepared and, if needed, discussed with the originator;
- Agreed changes will be integrated into a revised “Proposed Issue” version, which includes a summary of changes in the document record;
- The “Proposed Issue” will be consulted using appropriate working arrangements.

Note: Identified errors which may cause potential problems when implementing, may be corrected directly via a separate “Corrigendum”.



## ANNEX B – Security Monitoring

Chapter 7.4.2 of the ICAO AVSEC Manual [RD 3] describes four monitoring activities to verify regulatory compliance with the NCA, namely security audits, inspections, tests and surveys (see Table 9).

The new EASA basic regulation, Regulation (EU) 2018/1139 [RD 12], refers to “investigations, inspections, audits and other monitoring activities” (Article 62, 14a)), while Regulation (EU) 2017/373 [RD 8] is similar, but adds “assessments” (Article 5).

Monitoring Activity	Content	Characteristics	Notes
<b>Audit</b>	In-depth (as exhaustive as possible) examination of <b>all</b> aspects of the NCASP requirements	<ol style="list-style-type: none"> <li>1. Timing: from a number of days to one month</li> <li>2. Multi-site/location</li> <li>3. Should always be announced in advance</li> <li>4. Should not include overt or covert security tests</li> </ol>	Carried out by CA
<b>Inspection</b>	Examination of implementation of relevant provisions in the NCASP	<ol style="list-style-type: none"> <li>1. Narrower scope than an audit</li> <li>2. Focuses on a specific activity</li> <li>3. May be announced in advance</li> <li>4. May include overt or covert security tests</li> </ol>	Carried out by CA
<b>Test</b>	Simulation of an attempt to commit an unlawful act to test a security measure	<ol style="list-style-type: none"> <li>1. May be overt or cover security tests</li> <li>2. Only demonstrate if a security measure or control proved effective at a specific place and time</li> <li>3. Focus on access control to restricted areas, protection of assets, etc.</li> </ol>	Carried out by Entity, checked by CA
<b>Survey</b>	Evaluation of security needs	<ol style="list-style-type: none"> <li>1. Highlight vulnerabilities that could be exploited to carry out an act of unlawful interference</li> <li>2. Recommend corrective actions</li> <li>3. Should be carried out whenever a threat necessitates an increased level of security</li> <li>4. The scope ranges from targeted assessment of on a specific operation to an overall evaluation of security measures</li> <li>5. Timing: from a few hours to several weeks</li> <li>6. Should include overt or covert security tests</li> </ol>	Carried out by Entity, checked by CA

**Table 9 - Types of Monitoring Activities**

## ANNEX C – Compliance Classification Schemes

A number of compliance classification schemes for security in aviation exist, and a selection of these are described below. The ICAO scheme described in C.1 consists of 7 levels and is familiar to AVSEC professionals. The scheme described in C.2 is used for commission inspections in AVSEC, and uses 6 levels which can easily be mapped to the ICAO scheme.

C.4 describes the EASA scheme of Regulation (EU) 2017/373 [RD 8], which addresses safety oversight. This scheme consists of 3 levels.

### C.1 ICAO Doc 8973

The ICAO compliance classification scheme is shown in Table 10, and is described in detail in the AVSEC manual ([RD 3], section 7.4.4) which is specific to aviation security. ICAO's ATM Security manual [RD 5] states that the requirements of the AVSEC manual on the protection of Air Navigation Services should be incorporated in an ANSP's security programme. This classification scheme has 5 levels.

ICAO Doc 8973 (7.4.5)
a) Cat. 1: Meets the requirements
b) Cat 2: Does not meet the requirements and has minor deficiencies that need improvement
c) Cat 3: Does not meet the requirements and has serious deficiencies that need improvement
d) NA (not applicable): Measure or procedure does not exist at the given airport or is not available (e.g. off-airport check-in)
e) NC (not confirmed): Measure or procedure has been either not verified or not observed due to lack of time or other circumstances

**Table 10 – ICAO Doc 8973 – Compliance Classification Scheme**

### C.2 Regulation (EC) 72/2010

This regulation describes procedures for conducting commission inspections specifically in the area of aviation security in relation to Regulation (EC) 300/2008 [RD 10]. The classification scheme specified here is shown in Table 11. This scheme has 6 levels, and is very close to that described in the AVSEC manual [RD 3] and addressed in C.1.

<b>Regulation (EC) 72/2010 - Article 10</b>
a) Fully compliant
b) Compliant, improvement desirable
c) Not compliant
d) Not compliant with serious deficiencies
e) Not applicable
f) Not confirmed

**Table 11 – Regulation (EC) 72/2010 – Compliance Classification Scheme**

### C.3 Security Compliance Classification Scheme Mapping

Table 12 is an example of a possible mapping between two security compliance classification schemes for aviation security. If required, the development of such a mapping is the responsibility of the oversight authority.

<b>ICAO Doc 8973</b>	<b>Regulation (EC) 72/2010 - Article 10</b>
a) Cat. 1: Meets the requirements	a) Fully compliant
-	b) Compliant, improvement desirable
b) Cat 2: Does not meet the requirements and has minor deficiencies that need improvement	c) Not compliant
c) Cat 3: Does not meet the requirements and has serious deficiencies that need improvement	d) Not compliant with serious deficiencies
d) NA (not applicable): Measure or procedure does not exist at the given airport or is not available (e.g. off-airport check-in)	e) Not applicable

e) NC (not confirmed): Measure or procedure has been either not verified or not observed due to lack of time or other circumstances	f) Not confirmed
---	------------------

**Table 12 – Compliance Classification Scheme – Possible Mapping**

## C.4 Regulation (EU) 2017/373 Compliance Classification Scheme

The EU classification scheme is described in Regulation (EU) 2017/373 [RD 8] (*ATM/ANS.AR.C.050 Findings, corrective actions, and enforcement measures*) and is shown in *Table 13*. This scheme has 3 levels.

<b>Regulation (EU) 2017/373 (ATM/ANS.AR.C.050)</b>
Level 1: any serious non-compliance is detected with the applicable requirements
Level 2: any other non-compliance is detected with the applicable requirements
Observation: May be issued for those cases not requiring level 1 and 2 findings

**Table 13 – Regulation (EU) 2017/373 - Compliance Classification Scheme**

### 1. Level 1 Finding

A Level 1 finding represents a significant non-compliance with EASA regulatory requirements. Such a non-compliance could lower safety and security standards and adversely impact services.

This finding is issued by the CA when a significant non-compliance is detected with respect to one or more of the following:

- the applicable requirements of Regulation (EU) 2018/1139 [RD 12] and its Implementing Rules
- the organisation's procedures and manuals
- the terms of an approval or certificate
- the content of a declaration which lowers safety and security or presents a serious hazard to flight safety.

From Regulation (EU) 2017/373 ATM/ANS.AR.C.050, Level 1 findings include, but are not limited to, the following:

- (1) promulgating operational procedures and/or providing a service in a manner which introduces a significant risk to flight safety;

- (2) obtaining or maintaining the validity of the organisation's certificate by falsification of submitted documentary evidence;
- (3) evidence of malpractice or fraudulent use of the organisation's certificate; and
- (4) the lack of an accountable manager.

A resolution for a Level 1 finding should be provided immediately, by taking appropriate actions to prohibit or limit activities. If appropriate, the CA may revoke a certificate, an approval, or limit or suspend it, either in whole or in part, until successful corrective action has been taken by the organisation.

## 2. Level 2 Finding

A Level 2 finding may be one which lowers security and safety standards, represents a hazard to flight safety, or is a non-compliance with respect to Organisational Procedures.

Such a finding shall be issued by the Competent Authority when a non-compliance is detected with regard to:

- the applicable requirements of Regulation (EU) 2018/1139 [RD 12] and its Implementing Rules
- the organisation's procedures and manuals
- the terms of an approval or certificate
- the content of a declaration which could lower safety and security of operations or be considered a hazard to flight safety.

The Competent Authority shall grant the organisation a corrective action implementation period appropriate to the nature of the finding, but not exceeding 3 months. At the end of this period, and subject to the nature of the finding, the CA may extend the period, subject to agreement on a satisfactory corrective action plan.

Where an organisation fails to submit an acceptable corrective action plan, or to perform the corrective action within the time period accepted or extended by the CA, the finding shall be raised to Level 1, and action taken accordingly.

## 3. Observation

If there is no standard or requirement for an issue raised during the audit, this can be referred to in the report as an **Observation**. This is any item where objective evidence has identified potential problems that could lead to non-compliance.

## ANNEX D – Document Summaries

### D.1 ICAO

ICAO regulations are applicable globally to all ICAO member states. The following table provides information on these and applicable guidance material.

Document Title	Summary	Applicability
ICAO Annex 17 to the Convention on International Civil Aviation Security	First published in 1974, this outlines ICAO Standards and Recommended Practices (SARPs) for Aviation Security. Participating states were required to establish a National Civil Aviation Security Programme (NCASP) and supporting structures. The applicability of the NCASP was initially limited to aircraft operators and airports, focusing primarily on hijacking and bomb threats. Amendment 12 to Annex 17 (2010), required States to include Air Traffic Management (ATM) in the NCASP, and to ensure that Air Navigation Service Providers implement appropriate security provisions.	This is the main ICAO document for States on the organisation and implementation of the national aviation security system.  The only reference to ATM is the following article:  <i>Article 3.5 – Air traffic service providers</i>  <i>Each Contracting State shall require air traffic service providers operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State.</i>
ICAO Doc 8973 (Restricted) – Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference	The manual contains processes and procedures to assist States in preventing acts of unlawful interference and, if necessary, in response by developing the following elements:  - legal framework and control over ensuring security; - airport design, infrastructure and equipment; - recruitment, selection, preparation and certification of labour resources; - procedures and application of security measures.	This document is directed at security specialists.  It contains detailed guidelines for the implementation of the provisions of Annex 17. It is one of the main documents for the preparation, implementation and maintenance of the USAP-CMA.
ICAO Doc 9807 – Universal Security Audit Programme Continuous Monitoring Manual	This manual contains procedures, information and guidelines for the management and conduct of program activities under the USAP-CMA, which ensures that the security and monitoring systems implemented by States are continuously monitored.	This is one of the main documents containing the standardised USAP-CMA processes and procedures to ensure the systematic, uniform, objective and orderly preparation and conduct of activities and reporting on them.

<p>ICAO Doc 9985 (Restricted) – Air Traffic Management Security Manual</p>	<p>This manual provides guidance on security issues specific to ATM, in order to assist States and ATSPs in implementing appropriate security provisions to meet the published requirements of the NCASP.</p> <p>ATSPs also need guidance on the protection of ATM system infrastructure supporting international aviation.</p>	<p>This document is directed at security specialists.</p> <p>It contains guidelines specific to ATM for meeting the provisions of Annex 17. It is complementary to Doc 8973.</p> <p>It also provides guidance to the ATSP on the provision of ATM security services in support of national security and law enforcement requirements, and guidance on the protection of the ATM system infrastructure from threats and vulnerabilities.</p>
<p>ICAO Doc 10047, Aviation Security Oversight Manual – The Establishment and Management of a State’s Aviation Security Oversight System</p>	<p>This document is directed at high-level government decision makers. It outlines the duties and responsibilities of ICAO Member States with respect to the establishment and management of a national civil aviation security oversight system.</p> <p>This document identifies and explains the Critical Elements (CEs) involved in the establishment, implementation, and maintenance of a State’s civil aviation security oversight system, and supports the foundation of such a system.</p>	<p>This can be used as a supporting document for the USAP-CMA procedures, especially with regard to Critical Elements (CE) of the aviation security control system, which include:</p> <ul style="list-style-type: none"> <li>- the basic legislation in aviation security;</li> <li>- programs and rules for aviation security;</li> <li>- the relevant state authority for aviation security and its responsibilities;</li> <li>- personnel qualification and training;</li> <li>- providing technical advice, means and information critical to security;</li> <li>- obligations for certification and approval;</li> <li>- commitment to quality control;</li> <li>- solving problems in the field of aviation security</li> </ul>
<p>ICAO Doc 10108 – Aviation Security Global Risk Context Statement</p>	<p>This provides information on threats and risks facing civil aviation, and includes a methodology for States and aviation security stakeholders to conduct risk assessments.</p>	<p>Threat and risk information may be used to inform the risk management process, particularly the development of risk assessments.</p>

**Table 14 – ICAO Document Summaries**

## D.2 European Region

European regulations and directives are applicable in the European region. The following table provides information on these and applicable guidance material.

Document Title	Summary	Applicability
Regulation (EC) 549/2004, framework for the single European sky	The objective of the Framework regulation was to enhance safety standards and the efficiency of air traffic in Europe, to optimise system capacity and minimise delays by establishing a harmonised regulatory framework for air traffic management in Europe.	This introduces the need for a harmonised regulatory framework, which is subsequently reflected in regulations addressing ATM security.
Regulation (EU) 2017/373 common requirements for ATM/ANS	The regulation applies to ANSPs, the network manager and air traffic flow managers. It requires them to take the necessary measures to protect their systems, constituents in use, and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service.  Amended by Regulation (EU) 2020/469.	Specifies requirements for service providers to implement a security management system (including risk assessment, risk mitigation, monitoring, improvement, detection of breaches, and alerting of personnel), to ensure the security clearance of personnel, and coordinate with civilian and military authorities to ensure the security of facilities, personnel, and data.
Regulation (EU) 2020/469 common requirements for ATM/ANS	This regulation contains requirements for air traffic management/air navigation services, design of airspace structures and data quality, and runway safety. It repeals Regulation (EC) No. 73/2010, which was concerned with data quality. It amends Regulation (EU) 2017/373.	Amends Regulation (EU) 2017/373 particularly with respect to Aeronautical Information Systems. Amendments based on SARPS in ICAO Annex 15, Aeronautical Information Systems, Edition 16.
Directive 2008/114, on critical infrastructures and the need to improve their protection	This directive addresses the need for Member States to identify critical infrastructures, identify those which are European Critical Infrastructures (ECIs), and assess their needs for protection. Communications are required between ECI owners/operators, Member States and the Commission.	The directive applies to ECIs in all sectors, and introduces the need for ECIs to be assessed and protected, and for communications to be set up between States and the Commission.
Regulation (EC) No 300/2008 common rules in the field of civil aviation security	This regulation contains common rules in civil aviation security applicable to airports, airlines, and cargo. It includes passenger, baggage, cargo and mail screening, and the security of restricted areas.	Detailed implementing rules addressing this regulation are described in Regulation (EU) 2015/1998.



<p>Regulation (EU) No 72/2010 laying down procedures for conducting Commission inspections in the field of aviation security</p>	<p>This regulation provides procedures for conducting Commission inspections to monitor the application of Reg (EC) 300/2008.</p>	<p>In particular, Article 10 describes a classification scheme for use in assessments for compliance with Reg (EC) 300/2008.</p>
<p>Regulation (EU) No 628/2013 working methods for EASA for conducting standardisation inspections</p>	<p>This provides detailed implementing rules for conducting standardisation inspections.</p>	<p>The process described in this guidance document is elaborated from that described in this regulation, which is similar to the methodology proposed in ICAO Doc 8973 section 7.4.2.7.</p>
<p>Regulation (EU) 2015/1998 detailed measures for the implementation of the common basic standards on aviation security</p>	<p>Contained detailed implementing rules for 300/2008; repealed Regulation (EU) 185/2010, which had been amended 20 times since entering into force.</p>	<p>This act consolidated the initial act (300/2008) and all amendments.</p>
<p>Regulation (EU) 2019/1583 Cybersecurity measures</p>	<p>This amends 2015/1998 with regard to cybersecurity measures. It takes into account the following: the need to transpose ICAO Annex 17 standard 4.9.1; coordinates the application of the new rule if similar obligations are required from different legislative instruments.</p>	<p>Takes into account Annex 17 standard 4.9.1 and tries to address regulatory complexity.</p>
<p>Regulation (EU) 2018/1139 EASA Basic Regulation</p>	<p>This regulation lays down common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency. The regulation sets out the interdependency between civil aviation safety and security.</p>	<p>Requires that the EC, EASA, and Member States shall cooperate on security matters related to civil aviation, including cyber security, where interdependencies between civil aviation safety and security exist.</p>
<p>Regulation (EU) 2019/881 Cybersecurity Act</p>	<p>The act made ENISA a permanent EU agency, extended its mandate, and expanded its role in assisting and cooperating with national and European cybersecurity actors in the event of large-scale cyber incidents.</p>	<p>An entity which is categorized by a State as being a “provider of an essential service” is obliged to follow the requirements of the NIS Directive, and is subject to the requirements of the Cybersecurity Act. Consequently, the entity’s products, services and processes are subject to the European cybersecurity certification framework.</p>

	<p>It established a cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products, processes, and services.</p> <p>The Act complements the NIS Directive.</p>	
Directive (EU) 2016/1148 NIS Directive	<p>EU-wide legal framework on cybersecurity which addresses “providers of essential services”. Member States to adopt a national NIS strategy, creates a network of national Computer Security Incident Response Teams (CSIRT), and establishes security and notification requirements for digital service providers and operators of essential services</p>	<p>Notifications of security incidents with a significant impact on service provision should be provided to the NSA or CSIRT.</p> <p>ENISA acquired a mandate for the certification and oversight of ICT products, services and processes.</p>
EASA eRules for ATM/ANS	EASA eRules resource associated with Regulation (EU) 2017/373.	Provides information cross-referenced with other EU rules and regulations, as well as ICAO standards. References associated implementing rules, AMCs, and Guidance Material.
EASA eRules for the Basic Regulation	EASA eRules resource associated with Regulation (EU) 2018/1139.	As above.
ECAC Doc 30, Part II (Restricted)	Describes security provisions at national and airport level in addition to specific Baseline measures for securing airports, aircraft, passengers, cabin baggage, hold baggage, cargo and mail, in-flight supplies and airport supplies. Also includes provisions on in-flight security, ATM and cyber security and the management of threats and hijackings.	Contains high-level guidelines on both ATM and cybersecurity.
NEASCOG ATM Security Policy	Provides a high-level framework for the development and implementation of ATM Security.	A high level definition of topics to be addressed to ensure the security of a system or organisation.

**Table 15 – Summary of EU Legislation and European Regional Documents**

## ANNEX E – Applicable Requirements and Audit Team Skills

This section refers to applicable requirements from Regulation (EU) 2017/373 [RD 8] and its amendments, and describes the skills required within the Audit Team to carry out oversight activities.

Oversight inspectors and auditors must acquire necessary skills via an appropriate training programme (the NCASTP) to ensure that standards are maintained. They should also be independent from the entities being monitored.

### E.1 ATM/ANS.OR.B.005 Management system

The following general management system requirements, although not solely security-related, are nevertheless important pre-requisites for security, since they interact with security management and oversight activities.

ATM/ANS.OR.B.005 Management system		Audit Team Expertise Required
a)	A service provider shall implement and maintain a management system that includes:	Expertise in management system implementation, associated policies, and procedures. Knowledge of quality management (e.g. ISO 9001/EN 9100) may assist with oversight of the quality management elements of the management system.
	1) Clearly defined lines of responsibility and accountability throughout its organisation, including a direct accountability of the accountable manager.	Knowledge of how responsibilities and accountabilities are defined and communicated within a service provider and documented within the management system. Knowledge of the necessary attributes of accountable managers.
	2) A description of the overall philosophies and principles of the service provider with regard to safety, quality, and security of its services, collectively constituting a policy, signed by the accountable manager.	Knowledge of management system policies, in particular security management.
	3) The means to verify the performance of the service provider's organisation and the context in which it operates, which may affect established processes, procedures and services and, where necessary, change the management system and / or the functional system to accommodate those changes.	Expertise in management system implementation, associated policies, and procedures, and security performance monitoring and measurement.

	4) A process to identify changes within the service provider's organisation and the context in which it operates, which may affect established processes, procedures and services and, where necessary, change the management system and/or the functional system to accommodate those changes	Knowledge of processes which must be used by a service provider to identify proposed changes to the functional system, which may be driven by internal or external circumstances.
	5) A process to review the management system, identify the causes of substandard performance of the management system, determine the implications of such substandard performance, and eliminate or mitigate such causes	Expertise in management system assessment and improvement, to ensure continuing stability, adequacy, and effectiveness.
	6) A process to ensure that the personnel of the service provider are trained and competent to perform their duties in a safe, efficient, continuous and sustainable manner. In this context, the service provider shall establish policies for the recruitments and training of its personnel	Knowledge of the services provided and the training and competence requirements for personnel supporting service provision. Knowledge of records, including education, training, skills and experience
	7) Formal means for communication that ensures that all personnel of the service provider are fully aware of the management system that allows critical information to be conveyed and that makes it possible to explain why particular actions are taken and why procedures are introduced or changed	Knowledge of appropriate processes supporting communication of the effectiveness of the management system within a service provider.
b)	A service provider shall document all management system key processes, including a process for making personnel aware of their responsibilities, and the procedure for the amendment of those processes.	Knowledge of the requirements on a service provider to document its management system, which will typically include information such as the following : titles and names of nominated postholders; lines of responsibility; description and location of facilities; description of procedures for monitoring compliance referred to in ATM/ANS.OR.B.005(c).
c)	A service provider shall establish a function to monitor compliance of its organisation with the applicable requirements and the adequacy of the procedures. Compliance monitoring shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary.	Knowledge of compliance monitoring functions, their organisational set-up, documentation, and training requirements.
d)	A service provider shall monitor the behaviour of its functional system and, where underperformance is identified, it shall	Knowledge of performance indicators for functional systems. Knowledge of security-related issues impacting performance and their mitigation.

	establish its causes and eliminate them or, after having determined the implication of the underperformance, mitigate its effects	
e)	The management system shall be proportionate to the size of the service provider and the complexity of its activities, taking into account the hazards and associated risks inherent in those activities	Knowledge of the impact of the size, nature, and complexity of the activity of a service provider on the managements system.
f)	Within its management system, the service provider shall establish formal interfaces with the relevant service providers and aviation undertakings in order to	Knowledge of formal interfaces (e.g. service level agreements, letters of understanding, memorandum of cooperation) between service providers or between service providers and other aviation undertakings (e.g. aerodrome operators), for the identification of risks associated with the use of the services they provide.
	1) ensure that the aviation safety hazards entailed by its activities are identified and evaluated, and the associated risks are managed and mitigated as appropriate	Knowledge of the potential impact of security breaches on safety, and the identification, evaluation, and mitigation of associated risks.
	2) ensure that it provides its services in accordance with the requirements of this Regulation	Knowledge of service provision as it relates to this regulation.

**Table 16 - ATM/ANS.OR.B.005 Management system**

## E.2 ATM/ANS.OR.D.010 Security management

These are the primary security management requirements in the regulation.

ATM/ANS.OR.D.010 Security management requirements		Audit Team Expertise Required
a)	Establish a security management system to ensure:	Expertise in security management system implementation, associated policies, and procedures
	1) The security of their facilities and personnel and prevent unlawful interference with the provision of services	Expertise in securing facilities, including physical infrastructures, their perimeters, and supporting services such as power, water, HVAC, controlled entry systems, and communications systems. Knowledge of redundant systems and their use. Knowledge of potential threat actors, threats to service provision, and potential exploitable vulnerabilities.

	2) The security of operational data they receive, or produce, or otherwise employ, so that access is restricted only to those authorised	<p>Knowledge of the reception, transmission, and use of operational data, and its use by the service provider.</p> <p>Knowledge of potential physical and cyber threats.</p> <p>Knowledge of technical and procedural controls to restrict access to authorised personnel and systems.</p>
b)	The SeMS shall define:	
	1) Procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination	<p>Knowledge of the security risk assessment of facilities, ANS/ATM systems, and all supporting systems, addressing potential risks due to physical and cyber threats, and social engineering.</p> <p>Knowledge of implementing associated security controls (physical, technical, procedural, organisational) to mitigate risk.</p> <p>Knowledge of the Deming cycle (plan, do check, act), the iterative method to control and continuous improvement of the security management process.</p>
	2) The means designed to detect security breaches and to alert personnel with appropriate security warnings.	<p>Knowledge of monitoring means, systems, and procedures for the detection of physical and cyber breaches of facilities and systems. Knowledge of insider threats.</p> <p>Knowledge of alerting means, systems, and procedures related to physical breaches (e.g. CCTV, movement detectors, other sensors) and system breaches resulting from cyber attacks, potentially detected by SoCs and/or CERTs.</p>
	3) The means of controlling the effects of security breaches and to identify recovery actions and mitigation procedures to prevent re-occurrence	<p>Knowledge of the potential impact of breaches (physical, cyber), knowledge of mitigation means and procedures.</p>
c)	ANS, ATFM, and the NM shall ensure the security clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel, and data.	<p>Knowledge of security clearance standards and procedures within the State concerned.</p> <p>Knowledge of appropriate civil and military contacts for coordination purposes.</p>
d)	ANS, ATFM and the NM shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cybersecurity threats which may have an unlawful interference with the provision of their service.	<p>Knowledge of information security and cybersecurity threats and threat agents with respect to ANS, ATFM and NM systems.</p> <p>Knowledge of applicable mitigating controls.</p> <p>Knowledge of potential system and network vulnerabilities.</p>

**Table 17 - ATM/ANS.OR.D.010 Security management**

### E.3 ATM/ANS.OR.B.020 Personnel requirements

The following personnel requirements interact with security management and oversight activities.

ATM/ANS.OR.B.020 Personnel requirements		Audit Team Expertise Required
a)	A service provider shall appoint an accountable manager, who has the authority over ensuring that all activities can be financed and carried out in accordance with the applicable requirements. The accountable manager shall be responsible for establishing and maintaining an effective management system	Knowledge of security management systems, responsibilities, requirements, and the required authority of accountable managers.
b)	A service provider shall define the authority, duties and responsibilities of the nominated post holders, in particular of the management personnel in charge of safety, quality, security, finance and human resources-related functions as applicable.	Knowledge of the required authority, duties, and responsibilities of all staff involved in security management activities, particularly those in management roles.

**Table 18 - ATM/ANS.OR.B.020 Personnel requirement**

### E.4 ATM/ANS.OR.A.070 Contingency Plans

A contingency planning capability is a pre-requisite for resilience.

ATM/ANS.OR.A.070 Contingency Plans	Audit Team Expertise Required
A service provider shall have in place contingency plans for all the services it provides in the case of events which result in significant degradation or interruption of its operations	Knowledge of crisis management, coordination and communication with stakeholders, risk assessment, incident management

**Table 19 - ATM/ANS.OR.A.070 Contingency Plans**

## E.5 ATSEP.OR.105 Training and competence assessment programme

Air Traffic Safety and Electronics Personnel (ATSEP) must be appropriately trained in security issues to a level which is compatible with their roles and responsibilities.

<b>ATSEP.OR.105 Training and competence assessment programme</b>	<b>Audit Team Expertise Required</b>
<p>In accordance with point ATM/ANS.OR.B.005(a)(6), the service provider employing ATSEP shall establish a training and competence assessment programme to cover the duties and responsibilities to be performed by ATSEP.</p> <p>When ATSEP are employed by a contracted organisation, the service provider shall ensure that those ATSEP have received the applicable training and competences foreseen in this Subpart.</p>	<p>Knowledge of the training required by ATSEP to develop security knowledge and skills which are compatible with their roles and responsibilities. Knowledge of means of verification.</p>

**Table 20 – ATSEP.OR.105 Training and competence assessment programme**



## ANNEX F – Process Documents

The documents described in Table 21 are those which are recommended for use in the Oversight Process.

Document Title	Description
Annual Oversight Programme	The scope and schedule of oversight activities over a period of 12 months. Approved by the CA and the Entity.
Initiation Letter	This letter informs the Entity of an upcoming oversight activity, and summarises the legal basis.
Expectations	A description of the CA's expectations, including the type of monitoring activity, and elements to be addressed.
Oversight Programme	The scope and schedule of the upcoming oversight activities.
Evidence	All necessary information requested by the CA / Audit Team from the Entity. This may include copies or extracts from any document, record, or data held by or accessible to an Entity.
Questionnaires	Developed by the Audit Team during the Preparation phase, to be used during the on-site Execution phase during interviews of service provider personnel on any fact, document, object, procedure, or other relevant matter.
Checklists	Developed by the Audit Team during the Preparation phase, to be used during the on-site Execution phase during interviews of service provider personnel on any fact, document, object, procedure, or other relevant matter.
Audit Plan	A detailed schedule for on-site monitoring activities, allocating Audit Lots to each Audit Team member.
Audit Report	<p>The document records all oversight activities carried out, and includes the following information:</p> <ul style="list-style-type: none"> <li>• dates and locations of the oversight activities</li> <li>• the identification of the Entity</li> <li>• the composition of the Audit Team</li> <li>• identification of personnel interviewed</li> <li>• the objectives and scope of the audit</li> <li>• the audit schedule</li> <li>• findings and observations on compliance</li> </ul> <p>The following may be included as attachments:</p>

	<ul style="list-style-type: none"> <li>• documentation used to plan the audit</li> <li>• documentation reviewed during the audit</li> <li>• Checklists and Questionnaires used by the Audit Team</li> <li>• Evidence provided by the Entity (permission of the Entity required) findings and observations on compliance</li> </ul>
Action Plan	<p>The Action Plan addresses all Audit Findings and records the following:</p> <ul style="list-style-type: none"> <li>- a proposed corrective action which addresses the root cause</li> <li>- a proposed completion date</li> </ul> <p>High priority Actions are identified for completion as soon as is feasible</p>
Follow-up Audit Report	<p>This records the status of the corrective actions contained within the Action Plan. Completed actions are closed-out. A continuous oversight approach, where periodical Follow-Up reporting is carried out, is often considered to be better practice.</p>
Closure Letter	<p>This letter informs the Entity of the formal closure of the oversight activity once all the Audit Findings raised during a particular audit are closed</p>

**Table 21 – Oversight Process Documents**

## ANNEX G – Mapping of ATM/ANS.OR.D010 to Guidance Material

The following table maps the requirements in Regulation (EU) 2017/373 ATM/ANS.OR.D010 (Security Management Requirement) to the contents of guidance material in ECAC Doc. 30 Part II, ICAO Doc 9985, ICAO Doc 8973, and the CANSO Cybersecurity and Risk Assessment Guide [RD 28].

Chapter 13 of ECAC Doc 30 Part II is concerned with ATM Security, and related guidance is contained within Annex IV-13-A – ATM Security. Guidance material elements from this Annex is prefixed with “13-A-“.

Chapter 14 of ECAC Doc 30 Part II is concerned with Cyber Threats to Civil Aviation, and related guidance is contained within Annex IV-14-A – Guidance Material on Cyber Threats to Civil Aviation. Guidance material elements from this Annex is prefixed with “14-A-“.

The “Derived Components” column contains more detailed components associated with each requirement. They are provided as examples, and are neither definitive nor complete. Mappings such as this may be of use to ANSPs to assist them in self-assessment of compliance status, and may also be of use to Auditors.

Similar tables can be produced for other areas, such as Contingency Plans (E.4) and ATSEP training (E.5). The choice of guidance material and the selection of “Derived Components” may vary depending on the needs of the CA or the Entity.

ATM/ANS.OR.D.010 Security management requirements		Derived Components	ECAC Doc 30 Part II	ICAO Doc 9985	ICAO Doc 8973	CANSO Cyber Security and Risk Assessment Guide
a)	Establish a security management system to ensure:	Policy	13-A-9 SeMS components	Pt I 1.2.2 Risk-based security management Pt I 2.4 Policy Pt I 2.5 Structure, authority, responsibility Pt I 6 Contingency Planning	2.1.4 Primary objectives 9.3 SeMS 9.3.2.4 Mgmt commitment 9.3.2.9 Governance	3 Motives and Methods 7 Conclusions and recommendations
		Risk Assessment and Planning	13-A-9 SeMS components 13-A-10 Coordination	Pt I 6 Contingency Planning Appendix A Security risk management process	9.3 Threat & Risk Mgmt 9.3.4 Assessment 18 Cyber threats Appendix 37 Threat & Risk Assessment Methodology	3 Motives and Methods 6 Managing Cyber Risks – Assessing the risks to ATM systems 7 Conclusions and recommendations Appendix B – Risk Assessment Methodology

		Implementation and operation	13-A-9 SeMS components	Pt I 6 Contingency Planning Appendix A Security risk management process	17 Crisis management 18 Cyber threats	7 Conclusions and recommendations
		Checking and Corrective Action	13-A-9 SeMS components	Pt I 6 Contingency Planning Appendix A Security risk management process	9.3.5 Monitoring & improvement	7 Conclusions and recommendations
		Management Review	13-A-9 SeMS components	Pt I 6 Contingency Planning Appendix A Security risk management process	9.3.5 Monitoring & improvement	7 Conclusions and recommendations
		Training		Overview 2.3 NCASP Pt I 4 Personnel security Pt I 5 ICT System security	9.3.7 SeMS Training 18 Cyber threats	3 Motives and Methods – Training & awareness
	1) The security of their facilities and personnel and prevent unlawful interference with the provision of services	ATM Infrastructure (CNS), Facilities, Systems	13-A-17 Protection Inside, outside airport 13-A-18 3 <sup>rd</sup> party communications networks 13-A-19 Protection against security threats and vulnerabilities 13-A-20 Protection – location and criticality 13-A-21 Coordinate with airport operators	Overview 4.7 a) Safeguard ATM system Pt I 1.1.3, 1.1.4, 1.1.5 Infrastructure protection Pt I 3.2 Facility physical security and access control Appendix A 2.5	11 Airport security Appendix 37 Threat & Risk Assessment Methodology	
		Service continuity	13-A-14 Service continuity	Pt 1 6.1 Contingency planning	17 Crisis mgmt Appendix 37 Threat & Risk Assessment Methodology	3 Motives and Methods
		Provision of support	13-A-15 Support other authorities	Overview 4.7 b) Provide security services Overview 4.9 ATM security operations Pt 1 3.8 Dual requirements		
		Coordination	13-A-22 AAs, national authorities, airports 13-A-21 Coordinate with airport operators	Pt I 6.4.5 Neighbouring states	17 Crisis mgmt	

		Personnel security	13-A-26 Restrict access 13-A-27 Security checks 14-A-2.7 Remote access control	Pt I 4 Personnel security Pt I 4.3.4 Personnel screening and vetting Pt I 4.3.11 Visitor control	8 Selection, recruitment, training 11 Airport security	B.3 Dealing with the human threat
		Physical security	13-A-28 By design and protective measures 14-A-1. Prevent unauthorised access	Pt I 3.2 Facility Physical Security and Access Control Pt I 3.3 Layers of defence and mitigation options Overview 4.8 b) Protect facilities	11.2 Airport protection & access controls Appendix 18 Intrusion detection	4 Cyber Assets – Physical assets 5 Cyber Security in ATM – Mitigating physical attacks on cyber assets
		ICT Security	13-A-30 Protective measures for IT HW and SW 13-A-31 Protect Service-critical information against loss of CIA 13-A-32 Protect Service-critical systems 13-A-33 Protect Service-critical communications systems 14-A-1 Identify critical information systems 14-A-2.1 Protection of critical systems: authentication systems; access control; firewalls; virus protection 14-A-2.2 Threat assessment process 14-A-2.3 Network Separation 14-A-2.4 Responsibility 14-A-2.5 Security by design 14-A-2.6 Supply chain security 14-A-2.7 Remote access control 14-A-2.8 Cyberattack incident records	Overview 4.7 a) Safeguard ATM system Overview 4.8 a) Protect cyber systems Pt I 5 ICT System Security (including cybersecurity)	18 Cyber threats	4 Cyber Assets – Information systems 4 Cyber Assets – Data & information
	2) The security of operational data they receive, or produce, or	Service-critical information	13-A-31 Protect against loss of CIA 14-A-2.1 Protection of critical systems	Pt I 1.1.5 Infrastructure protection Pt I 1.2.3.2 Critical information	18 Cyber threats	4 Cyber Assets – Data & information 5 Cyber Security in ATM – Information sharing and handling

	otherwise employ, so that access is restricted only to those authorised			Pt I 2.4.5.1.2 Strategic security goals – information classification Overview 4.4 ATM-related information Overview 4.6 Other security services		
		Access control	14-A-2.1 Protection of critical systems: authentication systems; access control 14-A-2.3 Network separation	Pt I 3.2 Facility Physical Security and Access Control Pt I 3.3 Layers of defence and mitigation options Appendix B 4.9 – 4.12 Remote access	11.2 Airport protection & access controls 18 Cyber threats Appendix 18 Intrusion detection	2 Cyber Threats and Risks 4 Cyber Assets 5 Cyber Security in ATM – Mitigating physical attacks on cyber assets
b)	The SeMS shall define:					
	1) Procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination	Risk assessment	13-A-9 SeMS components 13-A-10 Coordination 14-A-1 Identify critical information systems 14-A-2.2 Threat assessment process; vulnerability assessment	Pt I 5.1.3 Risk management approach Appendix A Security risk management process Appendix B 3.2 Identify critical Cyber ICT systems	18 Cyber threats Appendix 37 Threat & Risk Assessment Methodology	Appendix B Risk Assessment Methodology
Risk mitigation		14-A-1 Application 14-A-2.1 Protection of critical systems 14-A-2.2 Establish mitigation measures	Pt I 3.3 Facility layers of defence and mitigation options Pt I 3.3.4 Mitigation options Pt I 5.3 ICT Security Controls Appendix A Security risk management process Appendix B 2.8 Cyber ICT Security Controls	18 Cyber threats Appendix 37 Threat & Risk Assessment Methodology	Appendix B Risk Assessment Methodology	
Security monitoring		13-A-9 SeMS components 14-A-2.2 Activity logs; alerting systems 14-A-2.8 Cyber attack incident records	Appendix A Security risk management process	18 Cyber threats	3 Motives and Methods Appendix B Risk Assessment Methodology	
Security reviews		13-A-9 SeMS components 14-A-2.8. Review of incident reports; analysis of incident records	Appendix A Security risk management process	17.15 Review, analysis & reports 18 Cyber threats	Appendix B Risk Assessment Methodology	

	2) The means designed to detect security breaches and to alert personnel with appropriate security warnings.	Detect security breaches	14-A-2.2. Activity logs; alerting systems	Pt I 1.2 Principles for infrastructure protection Pt I 3 Physical security	11.2 Airport protection & access controls 18 Cyber threats Appendix 18 Intrusion detection	3 Motives and Methods 6 Managing Cyber Risks Appendix A.3 NIST Cybersecurity Framework
		Alert personnel	Appendix B - 3 Cyber ICT Security Requirements, 3.4 Appendix C – ICT Security Controls, 2 Control categories	Pt I 5 ICT Security	18 Cyber threats Appendix 18 Intrusion detection	Appendix B.7 Sample risk assessment tables
	3) The means of controlling the effects of security breaches and to identify recovery actions and mitigation procedures to prevent re-occurrence	Response, recovery	6.3 Tactical Security Operations Appendix C – ICT Security Controls, Table C.7 Technical mechanisms and infrastructure, 6.1; Table C-8 Acquisition, development and maintenance, 7.15	Pt II 4 Disasters & public health emergencies	18 Cyber threats Appendix 18 Intrusion detection	
c)	ANS, ATFM, and the NM shall ensure the security clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel, and data.	Personnel clearance	13-A-27 Security checks	Pt I 4 Personnel security	8 Selection, recruitment, training	
		Coordination		Pt I 2 State responsibilities Pt I 6.2 Roles and responsibilities	5.2 NCASC 6.1.4 Coordination and communication 9 Threat & risk mgmt. 10.4.2 National armed forces 17 Crisis mgmt	
d)	ANS, ATFM and the NM shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cybersecurity threats	Identify critical information systems	14-A-1 Identify critical information systems	Appendix B 3.2 Identify critical Cyber ICT systems	18 Cyber threats Appendix 37 Threat & Risk Assessment Methodology	4 Cyber Assets B.1 Overview
		Protect critical information systems		Appendix B 3.3 – 3.6 Protect critical Cyber ICT systems	18 Cyber threats Appendix 37 Threat & Risk Assessment Methodology	4 Cyber Assets – Data & information
		Security by design		Appendix B 4.1 – 4.4	18 Cyber threats	3 Motives and Methods – design strategies

	which may have an unlawful interference with the provision of their service.	Network separation		Appendix B 4.5 – 4.8	18 Cyber threats	B.2 Threats & vulnerabilities – weak network controls A.3 NIST cybersecurity framework
		Remote access		Appendix B 4.9 – 4.12	18 Cyber threats	A.3 NIST cybersecurity framework
		Supply chain security		Appendix B 4.13 – 4.14	18 Cyber threats	B.2 Threats & vulnerabilities – supplier relationships

**Table 22 – Example Mapping of ATM/ANS.OR.D.010 to Guidance Material**



## ANNEX H – Check-list / Self-assessment Example

Table 23 is an example of how regulatory requirements and guidance material may be used for the development of check-lists (for CAs) or self-assessment questionnaires (for Entities). The “Expectations” are suggested examples, which have been obtained from the guidance material referenced in Table 22. Competent Authorities will establish their own Expectations. The additional columns are merely suggestions based on the oversight process described in this document. Multiple expectations should be addressed separately to simplify the activity.

ATM/ANS.OR.D.010 Security management requirements	Derived Components	Expectation	Means of Compliance	Evidence Available / Supplied	Compliance Assessment Result	Notes on “Findings”	Corrective Action Required	Proposed Completion Date	Additional Notes	
Notes :										
		Here, the expectations of the applicable regulations are described	Describe how the requirements are complied with. If an AMC has been applied, provide details.	Which evidence is provided to support compliance?	Does the available evidence provide confidence that the requirements are met? Document the finding level (1, 2, or observation)	Document the reasons for the selected Finding level.	Describe corrective actions required.	Provide proposed dates for the completion of corrective actions		
a)	Establish a security management system to ensure:	Policy	Policy endorsed by senior management							
			Specifies mission, vision							
			Specifies organisational structure, roles, responsibilities							
			Specifies strategic security goals							
			Specifies risk appetite							
			Specifies risk assessment triggers							
		...								
		Risk Assessment and Planning	A risk management process is established							
			Risk assessments are carried out on critical systems							
			...							
		Implementation and operation	The SeMS is operational							
			An incident management process is in place							
			Risk assessment triggers are specified;							
			Contingency procedures are specified;							
			...							
		Checking and Corrective Action	Continuous monitoring and improvement of the SeMS is carried out;							
			...							

		Management Review	The SeMS is under review (periodic, triggered)							
			Lessons are learned and disseminated							
			Improvements are implemented							
			...							
		Training	All staff are provided with security awareness training							
			A security culture exists							
			Specialist staff are provided with role-specific security training							
			...							
1)	The security of their facilities and personnel and prevent unlawful interference with the provision of services	ATM Infrastructure (CNS), Facilities, Systems	Risk assessments are performed							
			Critical infrastructure, facilities, and systems are identified							
			Risk assessments are correct, complete, and consistent with safety risk assessments							
			Residual risks are tolerable							
			Security controls are implemented (physical, personnel, ICT);							
			...							
		Service continuity	Security controls are in place to facilitate response and recovery							
			Contingency plans are in place							
			...							
		Provision of support	Systems and procedures are in place to support external stakeholders and authorities when required – e.g. military, search and rescue							
			...							
		Coordination	Systems and procedures are in place for coordination with national authorities, airports, and neighbouring states in normal and crisis situations							
			...							
		Personnel security	Staff undergo security training; remote; ...							
			Access to restricted areas depends on role							
			Access to systems is controlled							
			...							

		Physical security	Physical security by design is implemented									
			Access controls are implemented									
			Intrusion detection systems are operational									
			Physical access to ICT system physical assets is controlled to prevent unauthorized access									
			...									
			ICT Security	Risk assessments are carried out on all critical ICT HW and SW, and protective measures are in place; ; ...								
				Network separation is implemented;								
				Critical data and information are protected								
				Service-critical communications systems are protected								
				...								
	2) The security of operational data they receive, or produce, or otherwise employ, so that access is restricted only to those authorised	Service-critical information	Service critical data and information are identified and protected									
			Sharing of sensitive information is secured									
			...									
		Access control	Network separation is implemented									
			Physical security controls are implemented to mitigate physical access to cyber assets									
			Authentication systems are in place to limit access to authorized personnel									
			Intrusion detections are in place									
			...									
b)		The SeMS shall define:										
		4) Procedures relating to security risk assessment and mitigation, security monitoring and	Risk assessment	Risk assessment is carried out using a structured methodology; ;								
	Critical assets are identified;											
	Threat and vulnerability assessments are performed											
	...											
	Risk mitigation		Risks identified in risk assessment are mitigated by the implementation of security controls									

	improvement, security reviews and lesson dissemination		A holistic approach to controls is applied (defence-in-depth, -breadth)							
			...							
		Security monitoring	Critical systems are monitored incident alerts are generated							
			Intrusion detection systems (physical, cyber) are in place							
			Activity / incident logs are available;							
			...							
		Security reviews	Incident reports are reviewed and analysed							
			...							
5)	The means designed to detect security breaches and to alert personnel with appropriate security warnings.	Detect security breaches	Intrusion detection systems are in place (physical and cyber)							
			Anomalies in access control systems are detected							
			Activity logs are recorded;							
			...							
		Alert personnel	Appropriate personnel are alerted by intrusion detection systems (physical and cyber)							
			...							
6)	The means of controlling the effects of security breaches and to identify recovery actions and mitigation procedures to prevent re-occurrence	Response, recovery	Systems and procedures are in place to facilitate responding to, and recovering from, security breaches (physical and cyber)							
			Crisis management plans and procedures are in place							
			Personnel have been appropriately trained in desk-top exercises and/or simulations to perform effectively in non-nominal circumstances							
			...							
c)	ANS, ATFM, and the NM shall ensure the security	Personnel clearance	Personnel screening and vetting is performed during selection and recruitment							

	clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel, and data.		...								
		Coordination	Systems and procedures are in place to coordinate and communicate with relevant civil and military authorities								
			Crisis management procedures are in place supporting such coordination								
			...								
d)	ANS, ATFM and the NM shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cybersecurity threats which may have an unlawful interference with the provision of their service.	Identify critical information systems	Processes are in place to identify critical information systems								
			Threat / risk assessment methods are established								
			...								
		Protect critical information systems	Appropriate security controls are in place to mitigate identified risks								
			...								
		Security by design	Security is integrated into the design of systems during development								
			...								
		Network separation	Networks are separated to mitigate risk								
			...								
		Remote access	Remote access to systems is limited to authorised personnel								
			The access means is secure								
			...								
		Supply chain security	Providers of products and services must implement security controls to ensure the integrity of products or services delivered, the confidentiality of data exchanged, and the completeness of associated transactions								
			...								

**Table 23 – Example Table for Checklists or Self-assessment**



## SUPPORTING EUROPEAN AVIATION



© EUROCONTROL -

This document is published by EUROCONTROL for information purposes. It may be copied in whole or in part, provided that EUROCONTROL is mentioned as the source and it is not used for commercial purposes (i.e. for financial gain). The information in this document may not be modified without prior written permission from EUROCONTROL.

[www.eurocontrol.int](http://www.eurocontrol.int)



NETWORK  
MANAGER

