Council of the European Union

Brussels, 23 October 2025
(OR. en)

14417/25
ADD 1

AVIATION 143

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	15 October 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	D(2025) 109579 annex
Subject:	ANNEX to the COMMISSION REGULATION (EU) .../... of XXX amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as regards specifications for national quality control programmes in the field of civil aviation security

Delegations will find attached document D(2025) 109579 annex.

Encl.: D(2025) 109579 annex

EUROPEAN
COMMISSION

Brussels, XXX
D109579/02
[…](2025) XXX draft

ANNEX

ANNEX

to the

COMMISSION REGULATION

amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as regards specifications for national quality control programmes in the field of civil aviation security

ANNEX

"ANNEX II

COMMON SPECIFICATIONS FOR THE NATIONAL QUALITY CONTROL PROGRAMME TO BE IMPLEMENTED BY EACH MEMBER STATE IN THE FIELD OF CIVIL AVIATION SECURITY

1. DEFINITIONS

1.1. For the purposes of this Annex, the following definitions shall apply:

(1) 'annual traffic volume' means the total number of passengers arriving, departing and in transit (counted once);

(2) 'appropriate authority' means the national authority designated by a Member State pursuant to Article 9 to be responsible for the coordination and monitoring of the implementation of its national civil aviation security programme;

(3) 'auditor' means any person conducting national compliance monitoring activities on behalf of the appropriate authority;

(4) 'certification' means a formal evaluation and confirmation by or on behalf of the appropriate authority that a person possesses the necessary competencies to perform the functions of an auditor to an acceptable level as defined by the appropriate authority;

(5) 'compliance monitoring activities' means any procedure or process used for assessing the implementation of this Regulation and the national aviation security programme;

(6) 'deficiency' means a failure to comply with an aviation security requirement;

(7) 'inspection' means an examination of the implementation of security measures and procedures in order to determine whether they are being carried out effectively and to the required standard and to identify any deficiencies;

(8) 'interview' means an oral check by an auditor to establish whether specific security measures or procedures are implemented;

(9) 'observation' means a visual check by an auditor that a security measure or procedure is implemented;

(10) "overt test" means an announced exercise with screeners or other security personnel concerned which realistically simulates the performance of a security control or an act of unlawful interference for the purpose of examining or measuring elements such as the effectiveness of the implementation of existing security measures, competences and capabilities of that personnel to perform assigned functions;

(11) 'relevant authorities' means, for the purposes of Chapter 19, the appropriate authority or any other national authority having responsibilities for the reporting of aviation security occurrences, incidents, acts of unlawful interference and preparatory acts thereto;

(12) ‘reporter’ means any legal or natural person who reports a security occurrence, incident, act of unlawful interference, a preparatory act or other security-related information pursuant to the mandatory or voluntary reporting process established by Member States;

(13) ‘representative sample’ means a selection made from amongst possible options for monitoring which is sufficient in number and range to provide a basis for general conclusions on implementing standards;

(14) ‘security audit’ means an in-depth examination of security measures and procedures in order to determine if they are being fully implemented on a continual basis;

(15) ‘security incident’ means a security occurrence which affects or could affect the safety of passengers, crew, ground personnel and the general public;

(16) ‘security occurrence’ means any security-related event that may result in a reduced security outcome, may increase the operational risks or that endangers the safety of passengers, crew, ground personnel and the general public, or is a potential compliance breach. This includes the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference;

(17) ‘test’ means a trial of aviation security measures, where the appropriate authority simulates intent to commit an act of unlawful interference for the purpose of examining the effectiveness of the implementation of existing security measures;

(18) ‘verification’ means an action taken by an auditor to establish whether a specific security measure is actually in place;

(19) ‘vulnerability’ means any weakness in the implemented measures and procedures which could be exploited to carry out an act of unlawful interference.

2. POWERS OF THE APPROPRIATE AUTHORITY

2.1. Member States shall provide the appropriate authority with the necessary powers for monitoring and enforcing all requirements of this Regulation and its implementing acts, including the power to impose penalties in accordance with Article 21.

2.2. The appropriate authority shall perform compliance monitoring activities and have the powers necessary to require any identified deficiency to be rectified within set timeframes.

2.3. A graduated and proportionate approach shall be established regarding deficiency correction activities and enforcement measures. This approach shall consist of progressive steps to be followed until correction is achieved, including:

(a) advice and recommendations in writing;

(b) formal warning in writing;

(c) official enforcement notice;

(d) administrative sanctions and legal proceedings.

The appropriate authority may omit one or more of these steps, especially where the deficiency is serious or recurring.

3. OBJECTIVES AND CONTENT OF THE NATIONAL QUALITY CONTROL PROGRAMME

3.1. The objectives of the national quality control programme are to verify that aviation security measures are effectively and properly implemented and to determine the level of compliance with the provisions of this Regulation and the national civil aviation security programme, by means of compliance monitoring activities.

3.2. The national quality control programme shall include the following elements:

(a) organisational structure, responsibilities and resources;

(b) job descriptions of, and qualifications required for auditors;

(c) compliance monitoring activities, including scope of security audits, inspections, tests and, following an actual or potential breach of security, investigations, frequencies for security audits and inspections and also classification of compliance;

(d) surveys, where there is cause to reassess security needs;

(e) deficiency correction activities providing details concerning deficiency reporting, follow-up and correction in order to ensure compliance with aviation security requirements;

(f) enforcement measures and, where appropriate, penalties, as specified in points 2.1 and 2.3 of this Annex;

(g) reporting of compliance monitoring activities carried out including, where appropriate, information exchange between national bodies on compliance levels;

(h) monitoring process of the airport, operator and entity internal quality control measures;

(i) a process to record and analyse the results of the national quality control programme to identify trends and steer future policy development;

(j) a process for the mandatory reporting of information concerning aviation security incidents, acts of unlawful interference and preparatory acts thereto, by any operator and entity responsible for the implementation of the national civil aviation security programme in a practical and timely manner to the relevant authorities;

(k) a confidential, voluntary reporting system for analysing security information provided by sources such as the public, passengers, staff, crew, ground personnel and any other person in the aviation sector.

4. COMPLIANCE MONITORING

4.1. All airports, operators and other entities with aviation security responsibilities shall be regularly monitored to ensure the swift detection and correction of failures.

4.2. Monitoring shall be undertaken in accordance with the national quality control programme, taking into consideration the threat level, type and nature of the operations, standard of implementation, results of internal quality control of airports, operators and entities and other factors and assessments which will affect the priorities and frequency of monitoring.

4.3. Monitoring shall include the implementation and effectiveness of the internal quality control measures of airports, operators and entities.

4.4. Monitoring at each individual airport shall be made up of a suitable mixture of compliance monitoring activities and provide a comprehensive overview of the implementation of security measures in the field.

4.5. The management, setting of priorities and organisation of the quality control programme shall be undertaken independently from the operational implementation of the measures taken under the national civil aviation security programme.

4.6. Compliance monitoring activities shall include security audits, inspections and tests.

5. METHODOLOGY

5.1. The methodology for conducting monitoring activities shall conform to a standardised approach, which includes tasking, planning, preparation, on-site activity, the classification of findings, the completion of the report and the correction process.

5.2. Compliance monitoring activities shall be based on the systematic gathering of information by means of observations, interviews, examination of documents and verifications.

5.3. Compliance monitoring shall include both announced and unannounced activities.

6. SECURITY AUDITS

6.1. A security audit shall cover:

(a) all security measures at an airport; or

(b) all security measures implemented by an individual airport, terminal of an airport, operator or entity; or

(c) a particular part of the national civil aviation security programme.

6.2. A methodology for conducting a security audit shall be established taking into consideration the following elements:

(a) announcement of the security audit and communication of a pre-audit questionnaire, if appropriate;

(b) preparation phase including examination of the completed pre-audit questionnaire and other relevant documentation;

(c) entry briefing with airport/operator/entity representatives prior to beginning the monitoring activity on-site;

(d) on-site activity;

(e) debriefing and reporting;

(f) where deficiencies are identified, the correction process and the associated monitoring of that process.

6.3. In order to confirm that security measures are implemented, the conduct of a security audit shall be based on a systematic gathering of information by one or more of the following techniques:

(a) examination of documents;

(b) observations;

(c) interviews;

(d) verifications.

6.4. Airports with an annual traffic volume of more than 10 million passengers shall be subject to a security audit covering all aviation security standards at least every 4 years. The examination shall include a representative sample of information.

7. INSPECTIONS

7.1. The scope of an inspection shall cover at least one set of directly linked security measures of Annex I and the corresponding implementing acts monitored as a single activity or within a reasonable time frame, not normally exceeding three months. The examination shall include a representative sample of information.

7.2. A set of directly linked security measures is a set of two or more requirements as referred to in Annex I and the corresponding implementing acts which impact on each other so closely that achievement of the objective cannot be adequately assessed unless they are considered together. These sets shall include those listed in Appendix I to this Annex.

7.3. Inspections shall be unannounced. Where the appropriate authority considers that this is not practicable, inspections may be announced. A methodology for conducting an inspection shall be established taking into consideration the following elements:

(a) preparation phase;

(b) on-site activity;

(c) a debrief, depending on the frequency and the results of the monitoring activities;

(d) reporting/recording;

(e) correction process and its monitoring.

7.4. In order to confirm that security measures are effective, the conduct of the inspection shall be based on the systematic gathering of information by one or more of the following techniques:

(a) examination of documents;

(b) observations;

(c) interviews;

(d) verifications.

7.5. At airports with an annual traffic volume of more than 2 million passengers the minimum frequency for inspecting all sets of directly linked security measures set out in chapters 1 to 6 of Annex I shall be at least every 12 months, unless an audit has been carried out at the airport during that time. The frequency for inspecting all security measures covered by chapters 7 to 12 of Annex I shall be determined by the appropriate authority based on a risk assessment.

7.6. Where a Member State has no airport with an annual traffic volume exceeding 2 million passengers, the requirements of point 7.5 shall apply to the airport on its territory with the greatest annual traffic volume.

7.7. Frequencies for inspecting airports with an annual traffic volume not exceeding 2 million passengers, operators and entities shall be established by the appropriate authority taking into consideration the elements referred to in point 4.2. The frequencies shall refer to monitoring of all relevant sets of directly linked security measures set out in Chapters 1 to 12 of Annex I.

8. TESTS

8.1. Tests shall be carried out to examine the effectiveness of the implementation of the security measures listed hereunder, as a minimum at all airports falling under points 7.5 and 7.6:

(a) access control to security restricted areas;

(b) screening of persons other than passengers and items carried;

(c) aircraft protection;

(d) screening of passengers and cabin baggage;

(e) protection of hold baggage;

(f) screening of cargo or mail;

(g) protection of cargo and mail.

For tests to be performed at airports not falling under points 7.5 and 7.6, priorities shall be stablished in the yearly planning of compliance monitoring activities.

8.2. The appropriate authority may, on the basis of a risk assessment, carry out tests to examine the effectiveness of the implementation of the following additional security measures:

(a) examination of vehicles;

(b) aircraft security search;

(c) screening of hold baggage;

(d) screening of in-flight and airport supplies;

(e) protection of in-flight and airport supplies;

(f) protection of facilities and airport perimeter.

8.3. A test protocol including the methodology shall be developed taking into consideration the legal, safety and operational requirements. The methodology shall address the following elements:

(a) preparation phase;

(b) on-site activity;

(c) a debrief, depending on the frequency and the results of the monitoring activities;

(d) reporting/recording;

(e) correction process and the associated monitoring.

8.4. Frequencies for tests shall be established by the appropriate authority taking into consideration the elements referred to in point 4.2.

8.5. Tests may be replaced or supplemented by overt tests in cases where it is not possible to achieve a representative sample of tests due to, for instance, limited implementation of certain security measures, or when local conditions would impair the effectiveness of the tests.

9. SURVEYS

9.1. Surveys shall be carried out whenever the appropriate authority recognises a need to re-evaluate operations in order to identify and address any vulnerabilities. Where a vulnerability is identified, the appropriate authority shall require the implementation of protective measures commensurate with the threat.

10. REPORTING OF COMPLIANCE MONITORING ACTIVITIES

10.1. Compliance monitoring activities shall be reported or recorded in a standardised format which allows for an on-going analysis of trends.

10.2. The following elements shall be included in the standardised format:

(a) type of activity;

(b) airport, operator or entity monitored;

(c) date and time of the activity;

(d) name of the auditors conducting the activity;

(e) scope of the activity;

(f) findings with the corresponding provisions of the national civil aviation security programme;

(g) classification of compliance;

(h) recommendations for remedial actions, where appropriate;

(i) time frame for correction, where appropriate.

10.3. Where deficiencies are identified, the appropriate authority shall report the relevant findings to the airport, operators or entities subjected to monitoring.

11. COMMON CLASSIFICATION OF COMPLIANCE

11.1. Compliance monitoring activities shall assess the implementation of the national civil aviation security programme using the harmonised classification system of compliance set out in Appendix II.

12. CORRECTION OF DEFICIENCIES

12.1. The correction of identified deficiencies shall be implemented promptly. Where the correction cannot take place promptly, compensatory measures shall be implemented. When the overall monitoring of the implementation of a security measure, due to individual or isolated failures, results in the compliance level 'Compliant, but improvement desirable', those shortcomings shall also be corrected.

12.2. The appropriate authority shall require airports, operators or entities subjected to compliance monitoring activities to submit for agreement an action plan addressing any deficiencies outlined in the reports together with a timeframe for implementation of the remedial actions and to provide confirmation when the correction process has been completed.

13. FOLLOW-UP ACTIVITIES RELATED TO THE VERIFICATION OF THE CORRECTION

13.1. Following confirmation by the airport, operator or entity subjected to monitoring that any required remedial actions have been taken, the appropriate authority shall verify the implementation of the remedial actions.

13.2. Follow-up activities shall use the most relevant monitoring method.

14. AVAILABILITY OF AUDITORS

14.1. Each Member State shall ensure that a sufficient number of auditors are available to the appropriate authority directly or under its supervision for performing all compliance monitoring activities.

15. QUALIFICATION CRITERIA FOR AUDITORS

15.1. Each Member State shall ensure that auditors performing functions on behalf of the appropriate authority:

(a) are free from any contractual or pecuniary obligation to the airport, operator or entity to be monitored; and

(b) have the appropriate competencies, which include sufficient theoretical and practical experience in the relevant field.

Auditors shall be subject to certification or equivalent approval by the appropriate authority.

15.2. The auditors shall have the following competencies:

(a) an understanding of current applicable security measures and how they are applied to the operations being examined including:

– an understanding of security principles,

– an understanding of supervisory tasks,

– an understanding of factors affecting human performance,

(b) a working knowledge of security technologies and techniques;

(c) a knowledge of compliance monitoring principles, procedures and techniques;

(d) a working knowledge of the operations being examined;

(e) an understanding of the role and powers of the auditor.

15.3. Auditors shall undergo recurrent training at a frequency sufficient to ensure that existing competencies are maintained and new competencies are acquired to take account of developments in the field of security.

16. POWERS OF AUDITORS

16.1. Auditors carrying out monitoring activities shall be provided with sufficient authority to obtain the information necessary to carry out their tasks.

16.2. Auditors shall carry a proof of identity authorising compliance monitoring activities on behalf of the appropriate authority and allowing access to all areas required.

16.3. Auditors shall be entitled to:

(a) obtain immediate access to all relevant areas including aircraft and buildings for monitoring purposes; and

(b) require the correct implementation or repetition of the security measures.

16.4. As a consequence of the powers conferred on auditors, the appropriate authority shall act in accordance with point 2.3 in the following cases:

(a) intentional obstruction or impediment of an auditor;

(b) failure or refusal to supply information requested by an auditor;

(c) when false or misleading information is supplied to an auditor with intent to deceive; and

(d) impersonation of an auditor with intent to deceive.

17. BEST PRACTICES

17.1. Member States shall inform the Commission of best practices with regard to quality control programmes, audit methodologies and auditors. The Commission shall share this information with the Member States.

18. REPORTING OF COMPLIANCE MONITORING ACTIVITIES TO THE COMMISSION

18.1. Member States shall annually submit a report to the Commission on the measures taken to fulfil their obligations under this Regulation and on the aviation security situation at the airports located in their territory. The reference period for the report

shall be 1 January – 31 December. The report shall be due three months after completion of the reference period.

18.2. The content of the report shall be in accordance with Appendix III using a template provided by the Commission.

18.3. The Commission shall share the main conclusions drawn from these reports with Member States.

19. REPORTING OF AVIATION SECURITY OCCURRENCES, INCIDENTS, ACTS OF UNLAWFUL INTERFERENCE AND PREPARATORY ACTS THERETO

19.1. Where the appropriate authority identifies or receives information about an act of unlawful interference or an aviation security incident occurred or about to occur, which is having or likely to have a serious impact on the level of aviation security in the Union or on the international aviation security system, it shall inform the Commission as soon as possible. Subject to national rules on the protection of information relevant for national security, the notification shall include any relevant and available factual information useful to assess whether any prompt action is necessary in order to maintain or reestablish the level of aviation security in the Union and provide the necessary cooperation and coordination at international level. Upon receiving such information, the Commission shall inform the other Member States.

19.2. For the purpose of implementing the requirements laid down in points 3.2 (j) and (k) and the provisions hereunder, as from 1 January 2028 each Member State shall establish a process for the reporting, classification, processing, storage, protection, analysis and aggregation of information on aviation security incidents, acts of unlawful interference and preparatory acts thereto. That process shall provide for a mandatory and a confidential voluntary reporting systems and shall contain detailed requirements to ensure effective and efficient reporting and follow-up including the execution and coordination of subsequent tasks as well as any measures or decision that shall be taken by the relevant authorities.

19.3. As from 1 January 2028, operators and entities responsible for the implementation of the national civil aviation security programme shall report information on aviation security incidents to the relevant authorities. Security incidents are designated by a security official or manager to a reported security occurrence based on an analysis of the occurrence and a determination that additional action is required. A security incident may also result, and classified as such by the appropriate authority, in an act of unlawful interference to be reported to ICAO in accordance with Annex 17 to the Chicago Convention. The following reporting deadlines shall apply to such mandatory reporting, starting from the time when the underlying occurrence is reported through the internal reporting system referred to in point 19.4:

(a) as soon as possible, but within 24 hours at the latest in case the incident has a serious and immediate impact on the level of aviation security;

(b) within 72 hours, where the incident has a serious impact on the level of aviation security;

(c) on a monthly basis, in the case of all other incidents.

19.4. As from 1 January 2028, operators and entities responsible for the implementation of the national civil aviation security programme shall put in place an internal reporting system for the reporting of information on aviation security occurrences in a practical and timely manner. All personnel of operators and entities responsible for the implementation of the national civil aviation security programme shall report information on aviation security occurrences through such internal reporting system.

19.5. As from 1 January 2028, the relevant authorities and any operator or entity responsible for the implementation of the national civil aviation security programme shall designate at least one person or department responsible for reporting including data quality checking to improve data consistency. Recruitment and training requirements for the persons designated to perform such tasks shall be laid down in the implementing rules, adopted by the Commission in accordance with article 4(3) of this Regulation.

19.6. As from 1 January 2028, mandatory reporting to the relevant authorities shall be performed using the template as set out in Appendix IV, and shall refer to the common classification as laid down in Appendix V. Voluntary reporting may also be performed using the template set out in Appendix IV and refer to the common classification as laid down in Appendix V.

19.7. As from 1 January 2028*,* the relevant authorities shall store reports in a national database. The confidentiality of sensitive aviation security information contained in reports as well as any analysis thereof shall be ensured in accordance with applicable Union and national legislation. To this end, each Member State shall lay down detailed requirements regarding access to such information as well as its physical and information technology protection.

19.8. As from 1 January 2028, each Member State shall lay down detailed requirements on the processing and storage of reports to prevent the use of information contained therein for purposes other than aviation security and shall appropriately safeguard the confidentiality of the identity of the reporter and of the persons mentioned in the report, subject to the requirements on criminal, disciplinary or administrative proceedings under national law.

19.9. As from 1 January 2028, the relevant authorities shall establish and implement procedures for sharing, on a need-to-know basis, relevant information contained in reports and on follow-up actions to assist other national authorities and agencies, airport operators, air carriers and other entities concerned, where this may contribute to maintaining and improving aviation security.

19.10. As from 1 January 2028, notwithstanding point 19.8, in case the information has relevance for aviation safety, the relevant authorities may share it with the national civil aviation safety authorities, subject to the applicable requirements on confidentiality, protection and redaction as appropriate.

19.11. As from 1 January 2028, subject to the requirements on confidentiality and protection under Union and national legislation, as applicable, the relevant authorities shall share relevant information contained in reports with the Commission and other Member States, where this may contribute to maintaining and improving

aviation security, including in reply to specific queries by the Commission or other Member States.

19.12. As from 1 January 2028, subject to the requirements on confidentiality and protection under Union and national legislation, as applicable, the Commission and Member States may share relevant information contained in reports with international organisations and with the relevant authorities of third countries, where this is required under international agreements or where this may contribute to maintaining and improving aviation security.

19.13. As from 1 January 2028, without prejudice to points 19.1 and 19.11., Member States shall annually submit to the Commission a report containing statistics on the reports received, aggregated in accordance with the common classification as laid down in Appendix V and their analysis. The reference period for the report shall be 1 January – 31 December, and shall be due six months after completion of the reference period.

19.14. As from 1 January 2028, the Commission shall share the main conclusions drawn from reports submitted pursuant to point 19.13 with the Regulatory Committee for Civil Aviation Security and the Stakeholders Advisory Group on Aviation Security.

19.15. As from 1 January 2028, in order to provide a harmonised approach at Union level, the Commission may make available an appropriate information technology instrument to support the implementation of the requirements laid down in this Chapter, in coordination with Member States.

Appendix I

Elements to be included in the set of directly linked security measures

The sets of directly linked security measures as referred to in point 7.1 of this Annex shall include the following elements of Annex I and the corresponding provisions in its implementing acts adopted by the Commission in accordance with article 4(3) of this Regulation:

For point 1 — Airport security:

(a) all provisions of point 1.1; or

(b) all provisions of point 1.2 (except those relating to identification cards and vehicle passes); or

(c) all provisions of point 1.2 relating to identification cards; or

(d) all provisions of point 1.2 relating to vehicle passes; or

(e) all provisions of point 1.3 and the relevant elements of point 12; or

(f) all provisions of point 1.4; or

(g) all provisions of point 1.5; or

(h) all provisions of point 1.7, and the relevant elements of point 11.

For point 2 — Demarcated areas of airports:

all provisions of this point.

For point 3 — Aircraft security:

(a) all provisions of point 3.1; or

(b) all provisions of point 3.2.

For point 4 — Passengers and cabin baggage:

(a) all provisions of point 4.1 and the relevant elements of point 12: or

(b) all provisions of point 4.2; or

(c) all provisions of point 4.3.

For point 5 — Hold baggage:

(a) all provisions of point 5.1 and the relevant elements of point 12; or

(b) all provisions of point 5.2; or

(c) all provisions of point 5.3.

For point 6 — Cargo and mail:

(a) all provisions relating to security controls, screening and transportation applied by a regulated agent and the relevant elements of point 12; or

(b) all provisions relating to security controls and transportation applied by known consignors; or

(c) all provisions relating to security controls and transportation applied by approved hauliers; or

(d) all provisions relating to the protection of cargo and mail at airports.

For point 7 — Air carrier mail and air carrier materials:

all provisions of this point.

For point 8 — In-flight supplies:

all provisions of this point and the relevant elements of point 12.

For point 9 — Airport supplies:

all provisions of this point and the relevant elements of point 12.

For point 10 — In-flight security measures:

all provisions of this point.

For point 11— Staff recruitment and training:

(a) all provisions relating to staff recruitment at an airport, operator, air carrier or entity; or

(b) all provisions relating to staff training at an airport, operator, air carrier or entity.

Appendix II

Harmonised classification system of compliance

The following classification of compliance shall apply to assess the implementation of the national civil aviation security programme.

	Security Audit	Inspection	Test
Fully compliant	√	√	√
Compliant, but improvement desirable	√	√	√
Not compliant	√	√	√
Not compliant, with serious deficiencies	√	√	√
Not applicable	√	√	
Not confirmed	√	√	√

Appendix III

CONTENT OF REPORT TO THE COMMISSION

1. Organisational structure, responsibilities and resources

(a) Structure of the quality control organisation, responsibilities and resources, including planned future amendments (see point 3.2(a)).

(b) Number of auditors – present and planned (see point 14).

(c) Training completed by auditors (see point 15.2).

2. Operational monitoring activities

All monitoring activities carried out, specifying:

(a) type (security audit, initial inspection, follow up inspection, test, other);

(b) airports, operators and entities monitored;

(c) scope;

(d) frequencies; and

(e) total man-days spent in the field.

3. Deficiency correction activities

(a) Status of the implementation of the deficiency correction activities.

(b) Main activities undertaken or planned (e.g. new posts created, equipment purchased, construction work) and progress achieved towards correction.

(c) Enforcement measures used (see point 3.2(f)).

4. General data and trends

(a) Total national annual passenger and freight traffic and number of aircraft movements.

(b) List of airports by category.

(c) Number of air carriers operating from the territory by category (national, Union, third country).

(d) Number of regulated agents.

(e) Number of known consignors.

(f) Number of approved hauliers.

(g) Number of regulated suppliers (for airport supplies and for in-flight supplies).

(h) Approximate number of other entities with aviation security responsibilities (ground handling companies, security companies, known suppliers of airport and in-flight supplies).

5. Aviation security situation at airports

General context of the aviation security situation in the Member State.

Appendix IV

Template for the reporting of information on security occurrences and incidents[1]

Exact date and time or period[2] of occurrence: …/…/…

Date of the report:[3] …/…/…

Location of the occurrence[4]:

Name of the company and/or person reporting (if possible[5]):

Description of the occurrence:

Immediate action(s) taken and by whom:[6]

Affected area of aviation security:

Landside security; Passengers and cabin baggage; Staff and crew; Access control; Hold baggage; In-flight supplies; Airport supplies; Aircraft protection on the ground; Aircraft in-flight security measures; Cargo and mail; Air Traffic Control; Digital

1 For the purposes of the template, "occurrence" will cover aviation security occurrences and incidents.
2 In case the exact date and time cannot be established.
3 If different from the date of occurrence
4 Name and possibly IATA/ICAO code of the airport, as well as the area where the occurrence is observed
5 Name of natural person reporting may be left out.
6 Such as notifying local law enforcement and/or airport authorities of the situation.

information and technologies; Unmanned aircraft system(s) (UAS) / Unmanned aerial vehicle (UAV) / Remotely-piloted aircraft system(s) (RPAS); Stand-off weapon (MANPADs etc.); Lasers; Aviation security information; General Aviation/Aeroclubs

Effect or potential effect on security:[7]

Any other comment/proposal/information:[8]

Contact (email, telephone number):

Appendix V

Common classification of security occurrences and incidents[9]

Class[10]	**Category[11]**
Landside security	Discovery or use of vehicle-borne improvised explosive device (IED) or improvised incendiary device (IID)
	Discovery or use of person-delivered IED/IID
	Armed attack
	Unattended/suspicious items (also applicable airside)
	Chemical, biological and radiological (CBR) attack
	Damage to critical infrastructure/vulnerable points
	Suspicious behaviour

7 To determine from the reporter's perspective, how the level of aviation security is affected.

8 This section may include further desirable information from the reporter, for instance, as regards Preliminary risk assessment; Action(s) to limit the effect on aviation security; Remedial action(s) (where applicable); and Status of the file within the company (where applicable)

9 Appendix V may also serve as a tool to categorise security data and support the development of definitions of relevant occurrences.

10 Class: describes the topic the security incident would refer to, such as 'access controls', 'hold baggage' or 'cargo/mail'. The chosen identifiers are already commonly used in ICAO Annex 17 and the Aviation Security Manual (Doc 8973) and are expected to be easy for entities to refer to and relevant for authorities to make assessments.

11 Category: indicates a more specific description of the security incident involved. The categories differ per class as the possible security incidents vary depending on which aviation security process they relate to. For instance, the class 'aircraft protection on the ground' includes the category 'deficiency in the aircraft security search/check', whereas the class 'hold baggage' includes the category 'deficiency in protecting screened hold baggage'. There would also be a category 'other' for those incidents that may be too rare to justify a separate category, or which may be considered a new threat or vulnerability. However, this option should only be used when none of the other categories seems suitable.

	Unplanned disruptions, including bomb threat or hoax
Passengers and cabin baggage	Discovery or use of prohibited item/IED/IID
	Deficiency in the security checkpoint screening process
	Mixing of screened and unscreened passengers
	Suspicious behaviour
Staff and crew	Deficiency in the security checkpoint screening process
	Discovery or use of prohibited item/IED/IID
	Sabotage
	Insider bypassing security controls
	Deliberate attempt to circumvent vetting/background check regime
Access control	Breach or attempted breach of perimeter
	Unauthorized access to security restricted area (SRA) or other controlled area (non-staff)
	Unauthorized/unescorted access within SRA (staff)
	Suspicious behaviour of staff
	Deficiency in the access control system
	Deficiency in the ID pass issuing system
	Deficiency in the vehicle access control system including application of security controls and/or screening of occupants and vehicles
Hold baggage	Discovery or use of prohibited item/IED/IID
	Deficiency in protecting screened hold baggage
	Evidence of tampering of screened hold

	baggage
	Deficiency in the hold baggage screening (HBS) system or process (including passenger baggage reconciliation)
	Deficiency in the process of transportation of dispatched weapons
In-flight supplies	Unauthorized access to in-flight supply facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured in flight supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED/IID
Airport supplies	Unauthorized access to facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured airport supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED/IID
Aircraft protection on the ground	Unauthorized passenger on the aircraft
	Unauthorized staff on the aircraft
	Deficiency in the aircraft security search/check
	Deficiency in aircraft protection measures, including where aircraft are parked overnight
	Discovery or use of prohibited item/IED/IID in the aircraft cabin or hold
Aircraft in-flight security measures	Unruly passenger (to be considered for level 3 and 4 (see ICAO Aviation Security Manual) only to be reported)
	Deficiency in the cockpit door process/protection

	Discovery or use of prohibited item/IED/IID
	CBR attack
	Hijacking in flight
	Bomb threat in flight
Cargo and mail	Unauthorized access to cargo screening facility
	Deficiency in the screening process
	Discovery or use of prohibited item/IED/IID
	Deficiency in protecting secured cargo
	Evidence of tampering of secured cargo
	Deficiency in the acceptance process
	Suspicious activity
	Do Not Load notification under PLACI schemes
Air Traffic Control	Armed attack against air traffic control (ATC) facility
	Destruction or damage of air navigation aids
	Unauthorized access
Digital information and technologies	Attack against aircraft system(s)
	Attack against air traffic management (ATM) system(s)
	Attack against airport system(s)
	Attack against other critical systems and data
Unmanned aircraft systems (UAS) /	Unauthorized incursion into controlled airspace
Unmanned aerial vehicle (UAV) /	Near miss/Encounter with aircraft in flight
Remotely-piloted aircraft system (RPAS)	Strike/Collision with aircraft in flight
	Sighting from aircraft/airport
	Unmanned aerial vehicle (UAV) caused

	threat against aircraft
	UAV caused threat against airport infrastructure
	UAV caused threat against passengers
Stand-off weapon (MANPADs, etc.)	Attack on aircraft or airport facility
	Reported sighting
Lasers	Attack on aircraft or airport facility
	Reported sighting
	Suspicious activity
Aviation security information	Deficiency in protecting sensitive aviation security information
	Loss of integrity and availability of information systems
General Aviation/Aeroclubs	Unauthorized access
	Discovery of prohibited item/IED/IID

”