ECAC AVIATION SECURITY AUDIT AND CAPACITY BUILDING PROGRAMMES

2024 CATALOGUE

INTRODUCTION

The ECAC Aviation Security Audit and Capacity Building Programmes (ACBP) have been designed to support Member States to implement and oversee aviation security measures, and give them best practices, training and tools to further enhance their work in aviation security. The activities in the Programmes are designed to develop skills and competencies of national experts, and to share best practices for key aviation security areas such as compliance monitoring and vulnerability assessments. Under these Programmes, national experts and practitioners are made available as instructors, coaches and advisors, and provide practical advice to Member States looking to enhance their aviation security regimes.

Each year, ECAC advises its Member States on the activities offered. This Catalogue provides a single reference document for Member States to use throughout the year by presenting the wide range of activities offered. Each of the activities in the Catalogue is developed using European knowledge and expertise and can be tailored to meet your national needs and circumstances. ECAC can also develop additional activities should they be required to meet your specific needs.

TABLE OF CONTENTS

ECAC Aviation Security Audits

The ECAC Aviation Security Audit Programme is well known for its thoroughness and detailed approach.

The primary objective of the Programme is to assess the implementation of ECAC Doc 30, Part II (Security) Recommendations in ECAC Member States. As a more global objective, these audits contribute to more effective implementation of international aviation security standards by ECAC Member States and to the harmonisation of security measures among ECAC Member States. Participation in the Programme also facilitates the development of one-stop security arrangements in the ECAC region.

The following audits seek to identify areas of needed improvement and provide Member States with advice and technical expertise:

- National level: Aviation Security Audit of the Appropriate Authority
- Airport/entity level:
    o Full-Scale Aviation Security Audit of an Airport
    o Thematic Aviation Security Audit

All audit reports are classified as ECAC RESTRICTED and only given to the audited State.

Aviation Security Audit of the Appropriate Authority (national level)

Duration: 5 days

Participants: audit team (2 ECAC certified auditors)

Fee: none

Location: Member State

Objectives

The objectives of an ECAC aviation security audit of the Appropriate Authority are as follows:

- To assess the implementation of Doc 30, Part II Recommendations related to organisation of aviation security in a Member State;
- To verify the adequacy of compliance monitoring activities;
- To assess the effectiveness of compliance monitoring activities; and
- To verify the Appropriate Authority's regulatory functions in respect of:
  - Approval of regulated entities
  - Staff recruitment and training

Content

The main purposes of the audit at national level are to assess the national regulations and programmes and to verify the effectiveness of existing compliance monitoring systems in a Member State. Therefore, every national audit will be conducted in two parts:

- The first part which is carried out at the premises of the Appropriate Authority and covers the national regulations and programmes, and in particular, the implementation of the National Civil Aviation Security Quality Control Programme (NCASQCP) and the National Civil Aviation Security Programme (NCASP); and
- The second part is carried out at an airport which was recently subject to national compliance monitoring activities and which is representative of the country. The main aim of this part is to confirm the effectiveness of the implementation of the NCASQCP in the field.

Benefits

This audit provides a Member State with an internationally recognised, independent and objective evaluation of the content and implementation of national aviation security programmes focusing on the implementation of the national quality control programme.

An ECAC aviation security audit of the Appropriate Authority can also be used by Member States to prepare for ICAO audits and/or EC inspections or to identify areas that may benefit from capacity building activities. The report includes recommendations that a Member State may wish to introduce and provides a benchmark of performance within the ECAC region.

Full-Scale Aviation Security Audit of an Airport

Objectives

The objectives of an ECAC full-scale aviation security audit of an airport are as follows:

- To assess the implementation of **all Recommendations** of Doc 30, Part II, contained in Part Four (IV) Preventive Security Measures, including in-flight and ATM security, and Part Five (V) Management of Response to Acts of Unlawful Interference;
- To identify areas of needed improvement and provide advice and technical expertise;
- To contribute to the harmonisation of security measures among ECAC Member States; and
- To facilitate the implementation of one-stop security arrangements.

Content

An ECAC audit team will visit an airport nominated by the Appropriate Authority to assess whether or not all Doc 30 Recommendations are fully and properly implemented. If the audit team identifies deficiencies in the standards of implementation, they will attempt to identify the reasons for these deficiencies and will seek to assist the Appropriate Authority in achieving rectification; thus the Appropriate Authority and the regulated entity(ies) will be given the opportunity to receive adequate advice and technical expertise.

The full-scale audit results in the Interim Findings Report written on-site and the Final Audit Report submitted to the Appropriate Authority after the completion of the audit.

Benefits

This audit provides a Member State and its regulated entities with an internationally recognised, independent and objective verification of the implementation of all aviation security measures included in Doc 30, Part II.

A full-scale audit can be used by a Member State as an additional tool to its national compliance monitoring activities, to prepare for ICAO audits and/or EC inspections, or to identify areas that may benefit from further capacity building activities. Moreover, full-scale audits facilitate the development of one-stop security arrangements in the ECAC region and contribute to sharing knowledge and best practices among Member States.

Duration: 5-8 days depending on the size of the airport and the complexity of its operations.

Participants: audit team (2-6 ECAC certified auditors)

Fee: none

Location: Member State/airport

Thematic Aviation Security Audit (airport/entity level)

Objectives

The objective of an ECAC thematic aviation security audit is to evaluate the implementation of Doc 30, Part II Recommendations **in one or more domains of aviation security** at airport/entity level as agreed with the Appropriate Authority; to identify areas of needed improvement and provide advice and technical expertise.

Content

An ECAC audit team will visit an airport and off-airport entities (e.g. regulated agents and suppliers) nominated by the Appropriate Authority to assess whether or not recommendations contained in one or more chapters of Doc 30, Part II are fully and properly implemented.

A thematic audit may focus on one or more of the following domains:

- Airport security: airport planning, access control, screening of persons other than passengers and items carried, examination of vehicles, surveillance and patrols, demarcated areas;
- Aircraft security and in-flight security measures;
- Passenger and baggage security: screening and protection of passengers and cabin baggage; potentially disruptive passengers; screening and protection of hold baggage; passenger and baggage reconciliation;
- Cargo and mail security;
- Air carrier mail and materials, in-flight and airport supplies etc.

The scope of the thematic audit will be tailored to address the particular needs of a Member State or its airport. If an audit team identifies deficiencies in the standards of implementation, they will attempt to identify the reasons for these deficiencies and will seek to assist the Appropriate Authority in achieving rectification; thus, the Appropriate Authority and the regulated entity(ies) will be given the opportunity to receive adequate advice and technical expertise.

The thematic audit results in the Final Audit Report submitted to the Appropriate Authority after the completion of the audit. No Interim Findings Report is provided but a thorough oral debriefing at the end of the audit is given by the audit team.

Benefits

This audit provides a Member State and its regulated entities with an internationally recognised, independent and objective evaluation of the implementation of aviation security measures contained in a given chapter(s) of Doc 30, Part II. A thematic audit can be used by a Member State as an additional tool to its national compliance monitoring activities, to prepare for ICAO audits and/or EC inspections, or to identify areas that may benefit from further capacity building activities. Moreover, these audits facilitate the development of one-stop security arrangements in the ECAC region and contribute to sharing knowledge and best practices among ECAC Member States.

Duration: 3-6 days depending on the scope of the audit, size of the airport and complexity of its operations.

Participants: audit team (2-4 ECAC certified auditors)

Fee: none

Location: Member State/airport

TRAINING OF NATIONAL EXPERTS

The aviation security environment needs knowledgeable, skilled and competent professionals to prepare and conduct compliance monitoring activities.

The following activities seek to teach a range of skills and competencies to participants, from the conduct of inspections, to the organisation of covert tests. They are organised on site and include both classroom and practical exercises to maximise learning opportunities. Some activities can be delivered online (by videoconference) and can be completed by practical, on-site exercises.

Best Practices for National Auditors – Level 1

Objectives

Best Practices for National Auditors is an activity specifically tailored for national auditors. Through a combination of training techniques, including practical exercises at an airport, participants are familiarised with best practices in audit/inspection techniques. They will gain a better understanding of their role and responsibilities as national auditors and strengthen their experience and competency in conducting national compliance monitoring activities.

Content

Using experienced aviation security instructors, the Best Practices for National Auditors course comprises two groups of modules. The core modules introduce participants to inspection techniques and security technology, as well as compliance assessment and report writing. The second group, consisting of three modules, is selected by the Member State to reflect the training needs of its staff from the following list: inspecting aircraft security, inspecting passenger/baggage reconciliation, inspecting hold baggage security, and inspecting passenger and cabin baggage security. The course is tailored to the needs of each Member State. It includes classroom sessions and exercises, as well as on-site practical exercises.

Target group

Appropriate Authority representatives and other national auditors tasked with conducting quality control activities in the Member State.

Benefits

Participants are provided with theoretical and practical knowledge necessary to conduct national compliance monitoring activities in an efficient and standardised manner. On-site exercises provide an opportunity to benefit from the instructors' experience.

Duration: 5 days

Participants: max. 8 participants

Fee: course material free of charge. Instructors' costs may have to be covered in certain circumstances

Location: Member State/airport

Competencies to be acquired:
(Rec. 5.15.2 and Chapters 4, 5 and 12, Doc 30, Part II)

- an understanding of roles and powers of national auditors;
- an understanding of fundamental principles of compliance monitoring;
- an understanding of the manner in which national auditors should conduct themselves;
- an understanding of security measures, their objectives and applicability;
- knowledge of the types and scope of compliance monitoring activities;
- knowledge of the inspection/audit methodology and techniques;
- basic knowledge of the main security technologies, their capabilities and limitations;
- ability to identify and interpret the relevant European and national legal requirements in aviation security;
- ability to prepare for and to complete a comprehensive inspection of hold baggage security, passenger and cabin baggage security using the recommended approach; and
- ability to manage resistance and possible conflicts that may arise during compliance monitoring activities.

Best Practices for National Auditors – Level 2

Objectives

Best Practices for National Auditors – Level 2 builds on the experience and knowledge participants have gained from the training at Level 1. Accordingly, completion of Best Practices for National Auditors – Level 1 is recommended for participating in this activity. A combination of classroom presentations and practical activities at the airport ensures that participants can further develop their expertise in aviation security.

Content

To ensure participants gain the knowledge and expertise they need to operate at this level, experienced experts are provided by ECAC to instruct on this course. Topics covered include: assessing compliance, inspecting security equipment, and efficient documentation review, as well as a choice of two modules from the following: inspecting hold baggage, access control, airport supplies, in-flight supplies, cargo security, passenger/baggage reconciliation, aircraft security and passenger and cabin baggage security.

Target group

Appropriate Authority representatives and national auditors who have completed Best Practices for National Auditors – Level 1.

Benefits

Best Practices for National Auditors - Level 2 will enable auditors to further strengthen their competencies in the implementation of compliance monitoring activities. This course can also be considered as recurrent training for national auditors.

Duration: 3 days

Participants: max. 8 participants

Fee: course material free of charge. Course instructors' costs may have to be covered in certain circumstances

Location: Member State/airport

Competencies to be acquired:
(Rec. 5.15.2 and Chapters 1- 5, 8, 9 and 12, Doc 30, Part II)

- enhanced knowledge of the inspection/audit methodology and techniques;
- a better understanding of security measures, their objectives and applicability;
- knowledge of the European requirements for the operational deployment and use of security equipment;
- ability to prepare for and to complete a comprehensive inspection of access control, airport supplies and in-flight supplies security, passenger and baggage reconciliation, aircraft security, passenger and cabin baggage security using the recommended approach;
- ability to complete an inspection of security equipment deployed for aviation security purposes; and
- ability to complete an inspection of the use of Threat Image Projection.

Best Practices for Cargo Inspectors – Level 1 (basic)

Objectives

Best Practices for Cargo Inspectors Level 1 (basic) is an activity tailored towards national auditors who are tasked with conducting compliance monitoring activities (e.g. audits, inspections) in the field of cargo security and who need an initial training in this field. Through a combination of training techniques, including practical activities, participants acquire basic knowledge on the cargo security supply chain and audit/inspection techniques applied in cargo and mail security.

Content

The course presents the principles of cargo security and reviews some best practices that need to be applied in cargo audits and inspections. This includes an overview of cargo security measures and inspecting screening operations as well as, where applicable, the implementation of security measures throughout the cargo supply chain (e.g. inspecting a regulated agent). Last but not least, the course highlights and discusses the most common deficiencies in cargo security. This Level 1 course is not intended for experienced cargo inspectors.

Target group

Appropriate Authority representatives and other national auditors tasked with conducting quality control activities in the field of cargo and mail security.

Benefits

Participants are provided with theoretical and practical knowledge necessary to conduct cargo and mail security inspections in an efficient and standardised manner. The on-site practical exercises provide a unique opportunity to benefit from the instructors' experience in the field of cargo and mail security.

Duration: 3 days

Participants: 8 participants

Fee: course material free of charge. Instructors' costs may have to be covered in certain circumstances

Location: Member State

Competencies to be acquired:
(Rec. 5.15.2 and Chapters 6 and 12, Doc 30, Part II)

- an understanding of cargo operations and how the supply chain is organised;
- an understanding of threats and security measures applied to address such threats;
- knowledge of screening methods and security technologies, their capabilities and limitations;
- knowledge of cargo protection measures;
- ability to apply appropriate inspection methodology and techniques; and
- ability to prepare for and complete a comprehensive inspection of cargo security measures implemented by regulated agents and/or known consignors.

Best Practices for National Auditors – Cyber Security (basic)

Objectives

Best Practices for National Auditors – Cyber Security (Basic) aims to strengthen their understanding of cyber threats and cyber security measures, and include this component in their national compliance monitoring activities. This is an activity tailored for national auditors who are tasked with conducting compliance monitoring activities in the field of civil aviation cyber security.

Content

The course covers basic principles applicable for protecting critical aviation information and communications technology systems and data, used for civil aviation purposes, against cyber threats. These include an overview of international and European (ECAC/EU) requirements and recommendations for cyber security in civil aviation, common cyber threats to civil aviation, key players and their critical systems and data, basic principles of information security management system as well as cyber security organisational and protection measures. The course also covers best practices for inspecting cyber security measures in civil aviation.

The theoretical part of the course can be delivered online and can be completed by a practical, on-site activity at an airport.

Target group

National auditors/inspectors, who are not cyber security experts and are tasked with conducting quality control activities in the field of civil aviation cyber security and other representatives of the Appropriate Authority who are tasked with developing relevant procedures (manuals, handbooks).

Benefits

Participants are provided with basic theoretical and practical knowledge necessary to conduct national compliance monitoring activities in the field of civil aviation cyber security.

Duration: 3 days

Participants: max. 8 participants

Fee: course material free of charge. Course instructors' costs may have to be covered under certain circumstances

Location: online + on-site activity at an airport (optional)

Competencies to be acquired:

(Rec. 5.15.2 and Chapter 14, Doc 30, Part II)

- an understanding of cyber threats to civil aviation;
- an understanding of basic cyber security principles applicable to civil aviation;
- knowledge of international and European legal requirements relating to the protection of civil aviation against cyber threats;
- knowledge of applicable cyber security measures;
- ability to apply appropriate inspection methodology and techniques; and
- ability to prepare for and complete a comprehensive inspection of cyber security measures aimed to protect critical aviation systems against cyber threats.

Inspecting Cyber Security in Aviation (practical activity)

Objectives

The main objective of this activity is to enhance national auditors' understanding of the key cyber security measures in aviation and of good practices for inspecting/auditing their implementation. It also aims to provide national auditors with practical experience in inspecting/auditing cyber security measures in aviation, using a recommended approach.

Content

This activity is organised as a follow-up to the theoretical training course called Best Practices for National Auditors – Cyber Security (basic).

A combination of classroom presentations, discussions and practical activities at an airport ensures that participants can further develop their expertise in overseeing the implementation of cyber security measures in aviation. It comprises several activities focused on reviewing elements to inspect when collecting information on the protection of critical aviation information and telecommunication systems and data, used for aviation security purposes; preparation for an inspection/audit of cyber security measures, including drafting a checklist; on-site activities on inspecting cyber security of an airport operator and air carrier as well as an overview of potential deficiencies.

Target group

National aviation security auditors/inspectors, who are tasked with conducting quality control activities in the field of civil aviation cyber security.

Benefits

Participants are provided with theoretical and practical knowledge and experience necessary to conduct national compliance monitoring activities in the field of civil aviation cyber security.

Duration: 3 days

Participants: max. 8 participants

Fee: material free of charge. Instructors' costs may have to be covered under certain circumstances

Location: Member State

Competencies to be acquired:

(Rec. 5.15.2 and Chapter 14, Doc 30, Part II)

- a better understanding of the key cyber security principles applicable to civil aviation;
- knowledge of international and European legal requirements relating to the protection of civil aviation against cyber threats;
- knowledge of applicable cyber security measures;
- ability to identify and interpret the relevant European and national legal requirements in civil aviation cyber security;
- ability to apply appropriate inspection methodology and techniques; and
- ability to prepare for and complete a comprehensive inspection of cyber security measures aimed to protect civil aviation against cyber threats.

Recurrent Training for National Auditors

Objectives

Recurrent Training for National Auditors (RTNA) aims at strengthening the auditors' knowledge, understanding and competency in conducting national compliance monitoring activities on all chapters of ECAC Doc 30, Part II. Through a combination of theoretical training and table-top exercises, participants are familiarised with selected Doc 30 Recommendations (including the latest ones) and best practices in auditing/inspecting techniques.

Content

Using experienced aviation security instructors, the Recurrent Training for National Auditors course includes modules that provide national auditors with an opportunity to be reminded of security measures included in all chapters of ECAC Doc 30, Part II and to discuss on how best to inspect their implementation.

In order to practice and strengthen the participants' knowledge, every module is followed by a dedicated table-top exercise that enables participants to better understand the Doc 30 Recommendations and to put theory into practice.

Target group

Appropriate Authority representatives and other national auditors tasked with conducting quality control activities in the Member State.

Benefits

The role of each Appropriate Authority is to ensure that national auditors are provided with recurrent training enabling to acquire new competencies and strengthen the existing ones. Participating in a training provides a unique opportunity for national auditors to benefit from international expertise. The proposed training activity also contributes to the standardisation of national quality control activities.

Duration: 2-3 days

Participants: max. 8 participants

Fee: course material free of charge. Course instructors' costs may have to be covered under certain circumstances

Location: ECAC/Member State

Competencies to be acquired:

(Rec. 5.15.2 and Chapters 1-12, Doc 30, Part II)
- a better understanding of selected Doc 30 Recommendations (including the latest ones);
- knowledge of the inspection/audit methodology and techniques;
- an understanding of security measures, their objectives and applicability;
- ability to identify and interpret the relevant European and national legal requirements in aviation security;
- ability to prepare for and conduct inspections with regard to airport security, demarcated areas of airports, aircraft security, passengers and cabin baggie, hold baggage, cargo and mail, in-flight and airport supplies, security equipment; and
- ability to manage resistance and possible conflicts that may arise during compliance monitoring activities.
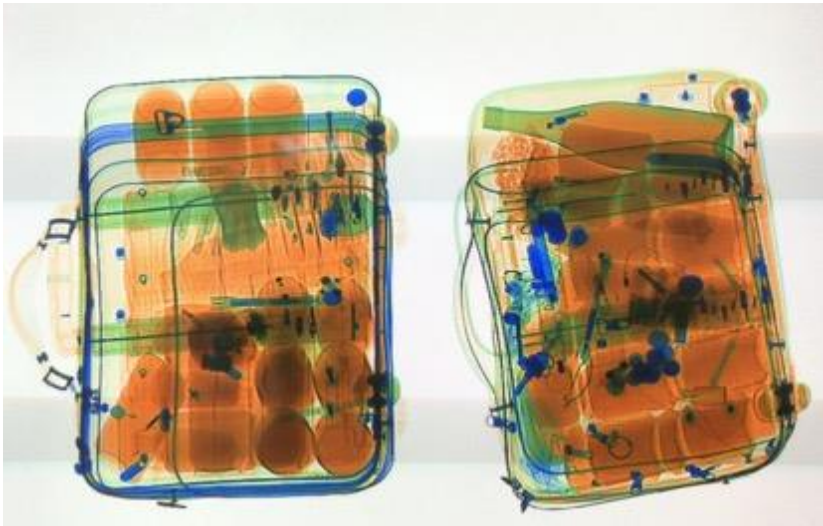
Best Practices on Covert Testing

Introduction

Member States clearly see the value of testing their aviation security regime to ensure its efficiency and robustness. However, conducting tests is challenging, and to ensure the objective of the test is achieved, appropriate test objects and procedures shall be used, and the analysis of results shall ensure that the overall security regime is improved.

Objectives

The purpose of the Best Practices on Covert Testing (BPCT) is to give Member States the necessary information, training and documentation to develop and implement their covert testing programme. This training is also intended for Member States that are looking to benchmark their covert testing procedures against international good practices.

Content

Best Practices on Covert Testing is an activity specifically tailored for national auditors who are tasked with developing or conducting covert tests in various fields of aviation security in the framework of the National Civil Aviation Security Quality Control Programme. Through a combination of training techniques, including practical activities, participants are familiarised with the key principles and good practices in covert testing techniques.

Target group

Appropriate Authority representatives and/or nominees responsible for conducting covert tests will gain most from this activity.

Benefits

Best Practices on Covert Testing enables Member States to develop or review their own covert testing programme and implement covert testing activities in a more standardised manner.

Duration: 3 days

Participants: max. 8 participants

Fee: course material free of charge. Instructors' costs may have to be covered under certain circumstances

Location: Member State

Competencies to be acquired:
(Rec. 5.15.2 and Chapters 1, 3-6 Doc 30, Part II)

- an understanding of the differences between covert and overt tests, their advantages and limitations;
- knowledge of testing methodology;
- knowledge of risk assessment principles related to the organisation and implementation of covert tests;
- knowledge of appropriate precautions to be employed when storing and transporting test items and when conducting tests;
- knowledge of test items for different areas of tests;
- ability to develop covert test protocols;
- ability to conduct covert tests according to the established protocol and using the recommended approach; and
- ability to interpret and analyse covert test results.

Best Practices for Drafting Technical Specifications for Security Equipment

Objectives

Best Practices for Drafting Technical Specifications for Security Equipment aims to strengthen technical knowledge in Member States and to support them in establishing and maintaining technical specifications and performance standards for security equipment as one of the key elements of the approval or certification of security equipment.

Content

This course is organised on a one-to-one basis, i.e. one State at a time, to focus on the State specific needs and questions. It presents an overview of the European requirements (ECAC/EU) for security equipment, an understanding on how to draft and interpret technical specifications/performance standards for all types of security equipment, key elements of the approval/certification process of security equipment, an understanding of capabilities and limitations of security equipment in detecting threat items and substances, and an understanding of the role of the ECAC Common Evaluation Process (CEP) of security equipment in supporting Member States, including interpreting CEP reports.

Following participation in the course, the State can be offered mentoring in establishing and updating its own technical specifications for security equipment.

Target group

Representatives of the Appropriate Authority who are tasked with approving/certifying security equipment, developing and maintaining national regulations and/or technical specifications for security equipment as well as overseeing the deployment of security equipment for screening.

Benefits

This course enables Member States to strengthen technical knowledge relating to security equipment and to establish and/or improve the approval/certification process of security equipment.

Duration: 2-3 days

Participants: max. 8 participants from one Member State

Fee: course material free of charge. Course instructors' costs may have to be covered under certain circumstances

Location: Member State or online + on-site mentoring activity (optional)

Competencies to be acquired:

(Rec. 5.15.2 and Chapter 12, Doc 30, Part II)

- enhanced knowledge of European (ECAC/EU) requirements for security equipment;
- a thorough understanding of technical specifications and performance standards provided by ECAC;
- ability to draft national technical specifications and performance standards for security equipment;
- knowledge of key elements of the approval/certification process of security equipment;
- a thorough understanding of capabilities and limitations of security equipment in detecting threat items and substances;
- an understanding of the role of the ECAC CEP of security equipment; and
- ability to understand and interpret CEP reports.

Best Practices for Inspecting Security Equipment

Introduction

Security equipment is one of the key elements of aviation security that strongly contributes to the protection of air transportation against acts of unlawful interference. Understanding the main elements of the efficient deployment of security equipment as well as its capabilities and limitations are essential to understand the proper implementation of aviation security measures.

Objectives

The main objectives of this training course are to familiarise participants with regulatory requirements in the field of security equipment, present limitations and capabilities of security equipment currently in use, as well as to provide good practices on inspecting security equipment.

Content

This course includes modules presenting European (ECAC/EU) requirements for security equipment, advantages and challenges of using different types of security equipment for different areas of aviation security, as well as best practices in inspecting the use of security equipment during national compliance monitoring activities.

Target group

National auditors tasked with conducting quality control activities on the use and deployment of security equipment.

Benefits

Best Practices on Security Equipment not only provides information on capabilities and limitations of security equipment but also enables to gain practical knowledge on inspecting the deployment of equipment at airports.

Duration: 3 days

Participants: max. 8 participants

Fee: course material free of charge. Course instructors' costs may have to be covered under certain circumstances

Location: Member State/airport

Competencies to be acquired:

(Rec. 5.15.2 and Chapter 12, Doc 30, Part II)

- an understanding of the role of the Appropriate Authority and regulated entities with regard to security equipment;
- knowledge of European (ECAC/EU) requirements for the deployment and use of security equipment;
- an understanding of capabilities and limitations of currently applicable security technologies;
- thorough knowledge of key elements to be covered when inspecting different types of security equipment;
- thorough knowledge of the applicable inspection methodology and techniques;
- an understanding of potential deficiencies relating to the deployment and use of security equipment;
- an understanding of routine testing procedures for security equipment; and
- ability to prepare for and to complete a comprehensive inspection of different types of security equipment, using the recommended approach.

Best Practices for Risk Management in Aviation Security

Objectives

Best Practices for Risk Management in Aviation Security aims to support Member States in applying a risk-based approach to aviation security, including risk-based security oversight, and in addressing current and emerging threats to civil aviation effectively.

Content

The course comprises two groups of modules. Through a combination of theoretical training, discussions and table-top exercises, the core modules familiarise participants with existing and emerging threats to civil aviation, current trends, risk management process, including a risk assessment methodology.

The second group of modules presents best practices for establishing and implementing risk-based security oversight and assessing risks in different areas of aviation, i.e. airport security, aircraft security, risks related to flights over and near conflict zones as well as risks posed by cyber threats and insiders. Particular attention is given to reviewing best practices for developing and implementing mitigating measures described in ECAC Doc 30, Part II (Security) to effectively address identified threats, using a risk-based approach. These modules may be selected by a Member State according to its needs.

Target group

This course is aimed at representatives of the Appropriate Authority and other national authorities (e.g. Ministry of Interior) tasked with conducting national risk assessment, developing and maintaining the National Civil Aviation Security Programme, national regulations and guidance material in the field of aviation security as well as planning of compliance monitoring activities.

Providing a valid security clearance (minimum level: ECAC/EU RESTRICTED) is a prerequisite for attending the course.

Benefits

Participants are provided with theoretical and practical knowledge necessary to develop and implement a national risk assessment methodology and develop effective mitigating measures.

Duration: 2-3 days

Participants: max. 8 participants

Fee: course material free of charge. Instructors' costs may have to be covered under certain circumstances

Location: ECAC offices/Member State

Competencies to be acquired:

(Chapters 2, 5 (Part III) and Chapters 1-9 and 14 (Part IV) of Doc 30, Part II)

- knowledge of current and emerging threats to civil aviation;
- knowledge of the risk management process, including the risk assessment methodology;
- knowledge of best practices for developing appropriate mitigating measures;
- ability to develop and implement a national risk assessment methodology;
- ability to assess risks to different areas of aviation: airport security, aircraft security, risks related to flights over/near conflict zones, risks posed by cyber threats and insiders, using a recommended approach;
- ability to develop effective mitigating measures; and
- ability to apply a risk-based approach to planning and conducting national compliance monitoring activities.

VULNERABILITY ASSESSMENTS

Security requires an understanding of threat, vulnerability, and risk. The ECAC vulnerability assessment process enables Member States to identify vulnerabilities in their aviation security systems, evaluate the effectiveness of existing mitigation measures, and receive good practices on the threat mitigation.

The vulnerability assessment process also ensures a transfer of knowledge to States' representatives so they can use the vulnerability tool again and again. Indeed, a State representative is invited to be a member of the ECAC team conducting the assessment.

Vulnerability Assessment – Landside Security

Introduction

Over the past years, there has been an increasing focus on compliance; matching operational practice to regulatory policies and procedures. However, from a security perspective it is possible to have a fully compliant system that remains vulnerable to attack. Security professionals recognise this and the vulnerability assessment process developed by ECAC is a tool available to Member States to help redress this issue.

Objectives

The purpose of an ECAC vulnerability assessment of landside security is to examine the threats and likely methods of attack in landside areas of an airport. Existing mitigation measures are assessed and good practices are offered to address any gaps.

Scope of the assessment

ECAC vulnerability assessments allow Member States to be proactive and get one step ahead. Assessments are conducted using ECAC certified assessors, together with a national representative who provides local knowledge and experience. In addition, the national representative learns the techniques and tools used in the process, so that at the end of the week-long process, this knowledge and expertise remains with the Member State and can be built upon and develop after the ECAC assessment team concludes.

The assessment looks at a wide variety of domains from the planning stage of airport infrastructure through to management of vehicles, operating practices and staff understanding of landside security.

Within one month of completion of the assessment on-site, Member States receive a comprehensive report indicating existing vulnerabilities and including good practices for mitigation of threats to landside areas.

Benefits

An ECAC vulnerability assessment enables Member State to review existing security measures implemented at landside areas of airports from a risk perspective. The full participation of the Appropriate Authority in the vulnerability assessment process ensures the transfer of knowledge and know-how.

Duration: 5 days

Participants: assessment team (3 certified assessors + representative of the Appropriate Authority)

Location: Member State/airport

Vulnerability Assessment – Insider Risks

Introduction

Over the past years, there has been an increasing focus on compliance; matching operational practice to regulatory policies and procedures. However, from a security perspective, it is possible to have a fully compliant system that remains vulnerable to attack. Security professionals recognise this and the vulnerability assessment process developed by ECAC is a tool available to Member States to help address this issue.

Objectives

The purpose of an ECAC vulnerability assessment of insider risks is to examine how insiders could exploit their knowledge or access to commit or facilitate an act of unlawful interference at an airport. Existing mitigation measures (e.g. establishment of a strong security culture) are reviewed and good practices offered to address any existing vulnerabilities.

Scope of the assessment

ECAC vulnerability assessments allow Member States to be proactive and get one step ahead. Assessments are conducted using ECAC certified assessors together with a national representative who provides local knowledge and experience. In addition, the national representative learns the techniques and tools used in the process, so that at the end of the week-long process, this knowledge and expertise remains with the Member State and can be built upon and developed after the ECAC assessment team concludes.

The assessment looks at a wide variety of domains from background and pre-employment checks, airport identification card systems, personnel security to staff perceptions, security culture.

Within one month of completion of the assessment on-site, Member States receive a comprehensive report indicating existing vulnerabilities and including good practices for mitigation against insider threats.

Benefits

An ECAC vulnerability assessment enables Member States to review existing security measures against insider threats implemented at State and at airport level from the risk perspective. The full participation of the Appropriate Authority in the vulnerability assessment process ensures the transfer of knowledge and know-how.

Duration: 5 days

Participants: assessment team (3 certified assessors + representative of the Appropriate Authority)

Location: Member State/airport

OTHER ACTIVITIES

Being a platform for the exchange of expertise and best practices in aviation security is one of the key objectives of ECAC. ECAC provides coaching activities on a bilateral basis to its Member States on a range of aviation security topics, using its network of experts.

Using the achievements and experience of Member States and the works of its study groups, ECAC can facilitate the organisation of activities between its States in order to share best practices.

Basic Aviation Security Training

Objectives

Basic Aviation Security Training is an activity specifically tailored for newly appointed national auditors and representatives of Appropriate Authorities involved in policy making. Through a combination of presentations and theoretical exercises, they will gain a better understanding of history of civil aviation security, international organisations and cooperation in the field of aviation security and role and responsibilities of Appropriate Authorities in this field.

Content

Using experienced aviation security instructors, the Basic Aviation Security Training course comprises two groups of modules. The introductory modules provide participants with an overview of threats against civil aviation, aviation security incidents and consequences they had for the development of aviation security measures, role and responsibilities of international and European organisations including ICAO, ECAC and EU. The second group of the modules provides an overview of existing security measures focusing on their security objectives and the different ways of their implementation.

The training course comprises classroom session and exercises.

Target group

Newly designated staff of the Appropriate Authority and national auditors tasked with developing policy and/or conducting quality control activities in the Member State.

Benefits

Appropriate Authority staff is provided with knowledge about aviation security organisation at international and national level. Good understanding of the history of aviation security, the role and responsibilities of Appropriate Authorities will enable newly designated security experts to put their activities in the wider context of civil aviation security.

Duration: 2 days

Participants: max. 10 participants

Fee: course material free of charge. Instructors' costs may have to be covered in certain circumstances

Location: ECAC/Member State/online

Competencies to be acquired:
(Chapters 1-14, Doc 30, Part II)

- knowledge of the history of attacks against civil aviation;
- an understanding of threat scenarios and the reasons for establishing different security measures;
- knowledge of the key principles of risk assessment in aviation security;
- an understanding of the organisation of aviation security at international, European and national levels;
- an understanding of the role of the Appropriate Authority in the aviation security system;
- basic knowledge of the key aviation security measures, their objectives and applicability; and
- basic knowledge of the deployment and use of security equipment.

COMMON EVALUATION PROCESS OF SECURITY EQUIPMENT

CEP Awareness Training

Objectives

CEP Awareness Training aims to provide ECAC Member States with a better understanding of the ECAC Common Evaluation Process (CEP) of security equipment and its role in supporting Member States.

Content

This activity is part of a process to develop technical expertise in ECAC Member States and is related to other ECAC activities such as establishment and improvement of technical specifications and performance standards for security equipment; development of common testing methodologies for security equipment, laboratory testing of security equipment against ECAC/EU performance standards; organisation of workshops and training courses on security equipment.

It comprises two theoretical sessions covering an overview of legal basis for establishing CEP, its objectives, benefits and deliverables, key principles and main actors involved in implementing CEP. Through a combination of theoretical presentations and a virtual activity, participants are also familiarised with the types of security equipment covered by CEP, types of tests conducted within the framework of CEP, an overview of a testing process, communication of test results, including the role of "CEP designees". Particular attention is paid to understanding and interpreting CEP reports.

Target group

This activity is preliminary opened for "CEP designees" (persons designated to receive CEP test reports), heads of aviation security departments/sections and security experts involved in approval/certification of security equipment at national level.

Benefits

This activity enables Member States to strengthen technical knowledge relating to security equipment and to better understand the role of the CEP, in particular its deliverables.

Duration: 2 days

Participants: max. 20 participants

Fee: none

Location: online

National Inspectors' Exchange Programme

Objectives

The National Inspectors' Exchange Programme is an activity designed for national inspectors with at least two years' experience of conducting compliance monitoring activities (e.g. audits, inspections) in their own State.

The programme allows States to facilitate inspector learning and development, as well as enable learning to adapt to changing aviation contexts e.g. different regulatory approaches, methods of screening that the inspector would not have in their own State, as well as best practices that they can learn from and embed in their national systems. Additionally, for the participating inspectors, specialists can get involved in inspections in other domains, generalists can broaden their experience base and gain valuable experience working in an international context, as well as affording participants an opportunity to build up their international peer network.

Content

The exchange is facilitated by the ECAC Secretariat. Each State can volunteer to host and to participate by nominating inspectors for the programme based on their learning and continuous professional development needs. The Secretariat matches hosts and participants. The host State is responsible for arranging the dates, facilitating an entry briefing to introduce the national process, before going into the field to conduct inspections with the nominated participant in their capacity as an observer. The participant is subject to a Code of Conduct, engages in the compliance activities and prepares a report for ECAC detailing their learning outcomes. ECAC can use the reports to identify common learning needs and develop specialist training accordingly.

Target group

Appropriate Authority representatives and other national auditors tasked with conducting quality control activities in the field of aviation security.

Benefits

Through a combination of peer learning and participation in audits/inspections in another State, the participants gain valuable expertise and exposure to learning opportunities that would otherwise not be available to them.

Duration: 3-5 days

Fee: Participants costs to be covered by own State

Location: Member State

Mentoring Activity on Behaviour Detection

Introduction

Mentoring activity on behaviour detection is an activity during which a Member State with an active Behaviour Detection (BD) Programme supports another State in the development and deployment of a BD Programme by sharing its expertise and achievements in this field.

The request for a mentoring activity requires a political commitment from the State applying for the mentoring activity, together with the confirmation of the availability of the required resources for behaviour detection. The mentoring activity is implemented directly by a mentor (a State) appointed by the ECAC Behaviour Detection Study Group.

Objectives

The objectives of this activity are to:

- Exchange the experience and expertise in the field of behaviour detection;
- Develop a BD Programme to be implemented in the State concerned; and
- Train the behaviour detection officers or provide guidelines in this field, depending on the required assistance.

Content

The focus is on the development of a national BD Programme for a Member State, training of behaviour detection officers and on setting the capabilities to be used for the oversight functions once the BD Programme is in place.

Benefits

Implementation of behaviour detection provides an additional layer of security. Member States with an active BD Programme are invited to join the ECAC Behaviour Detection Study Group, and benefit from the Member States' experiences and developments.

Duration: 3 months to one year

Fee: none

Location: ECAC offices/Member State + on-site mentoring

Mentoring Activity on Explosive Detection Dogs

Duration: flexible

Fee: none

Location: ECAC Member State(s)

Introduction

Mentoring activity on explosive detection dogs aims to support Member States in the development and deployment of explosive detection dog programmes in aviation security.

The mentoring activity is implemented directly by a mentor (an authority or persons) appointed by the ECAC Study Group on Explosive Detection Dogs.

Objectives

The objectives of this activity are to:

- Exchange the experience and expertise in the field of explosive detection dogs;
- Develop an EDD programme to be implemented in the State concerned; and
- Train the explosive detection dogs authorities' officials or provide guidelines in this field, depending on the required assistance.

Content

The focus is on the development of a national EDD programme and certification scheme. Similarly important part of the activities is to explore new applications of EDDs (i.e. screening of persons, examination of vehicles) and EDD limiting conditions.

Benefits

EDDs are effective means of screening mainly in cargo industry, but also in other areas where EDDs can be used as additional layer of aviation security. However, this method has also its limits and each Member State should be well aware of them before setting up the EDD programme. By implementing a mentoring activity, the ECAC Study Group on Explosive Detection Dogs seeks to extend EDDs programme within the ECAC region for the benefit of aviation security.