

**Manual for National  
ATM Security Oversight**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>03 October 2013</b>
<b>Status</b>	<b>:</b>	<b>Released Issue</b>
<b>Intended for</b>	<b>:</b>	<b>Restricted</b>

## DOCUMENT CHARACTERISTICS

TITLE		
<b>Manual for National ATM Security Oversight</b>		
<b>Document Identifier</b>	<b>Edition Number:</b>	2.0
	<b>Edition Date:</b>	03 October 2013
<b>Abstract</b>		
<p>This manual provides guidance to the national authorities responsible for aviation and ATM security on:</p> <ul style="list-style-type: none"> <li>- the understanding, context and scope of ATM security and its interfaces with the broader aviation security;</li> <li>- how to carry out the oversight of ATM security management systems;</li> <li>- how to be prepared for external ATM security oversight e.g. in the context of ICAO, ECAC and EASA audits or inspections.</li> </ul> <p>The first part of the document (main body) is dedicated to the first bullet point above, in order to support national authorities understanding the complexity and components of ATM security. Bullet points 2 and 3 are mainly developed throughout the questionnaires included in the annexes to the manual.</p>		
<b>Keywords</b>		
Appropriate Authority	ATM security	aviation security
governance	manual	National Civil Aviation Security Programme
National Supervisory Authority	oversight	Security questionnaire
cyber security	National Civil Aviation Security Quality Control Programme	
<b>Contact Person(s)</b>	<b>Tel</b>	<b>Unit</b>
Antonio NOGUERAS	(32) 2 729 46 69	DSS/CM/SEC

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


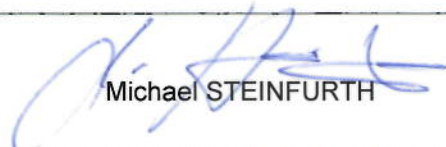
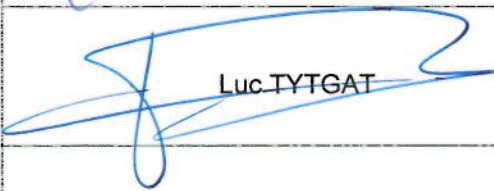
ELECTRONIC SOURCE		
Path:	H:\DSS-CMAC\EUROCONTROL\CMAC\DSS-CM-SEC\Deliverables\Manual for National ATM Security Oversight V2 0.doc	
Host System	Software	Size
Windows_NT	Microsoft Word 2002	2356 Kb

**Publications**  
 EUROCONTROL Headquarters  
 96 Rue de la Fusée  
 B-1130 BRUSSELS

Tel: +32 (0)2 729 4715  
 Fax: +32 (0)2 729 5149  
 E-mail: [publications@eurocontrol.int](mailto:publications@eurocontrol.int)

**DOCUMENT APPROVAL**

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Head of Unit DSS/CM/SEC	 Antonio NOGUERAS	02/10/2013
Head of Division DSS/CM	 Michael STEINFURTH	02/10/2013
Director Single Sky	 Luc TYTGAT	02/10/2013

## DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	10/10/2012	Creation	All
2.0	03/10/2013	Update	All

# CONTENTS

<b>DOCUMENT CHARACTERISTICS</b> .....	<b>ii</b>
<b>DOCUMENT APPROVAL</b> .....	<b>iii</b>
<b>DOCUMENT CHANGE RECORD</b> .....	<b>iv</b>
<b>LIST OF FIGURES</b> .....	<b>viii</b>
<b>LIST OF Tables</b> .....	<b>ix</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>1</b>
<b>1. Introduction</b> .....	<b>2</b>
<b>2. Aim</b> .....	<b>3</b>
<b>3. Scope</b> .....	<b>5</b>
3.1 Holistic Approach.....	5
3.2 Understanding Aviation Security (AVSEC).....	6
3.2.1 AVSEC Protection Layers.....	7
3.3 Understanding ATM Security.....	9
3.4 The Transversal Security Measures.....	10
3.5 Cyber Security.....	10
3.5.1 Critical Infrastructure Protection.....	11
3.5.2 The Cyber Threat.....	12
3.5.2.1 Concepts.....	12
3.5.2.2 Threat Classification.....	13
3.5.2.3 Threat Agents.....	14
3.5.2.4 Threat Assessment.....	15
3.5.2.5 Building Cyber Resilience.....	17
3.5.2.6 Specific Key Findings Regarding Cyber Security and Cyber Resilience.....	18
<b>4. Policy and Strategic Planning</b> .....	<b>20</b>
4.1 Mission.....	20
4.2 Vision.....	20
4.3 Strategic Objectives.....	20

4.4	ATM Security Principles .....	21
4.5	Fragmentation Analysis.....	21
4.6	Education, Awareness and Training .....	21
4.7	Safety/Security Interface .....	23
4.8	Threat and Risk Assessment .....	24
4.9	Cost and Benefits of Security.....	26
4.10	Crisis Management .....	27
4.11	International Collaboration, Civil-Military Coordination .....	27
<b>5.</b>	<b>Regulatory Framework .....</b>	<b>28</b>
5.1	The Global Regulatory Framework.....	28
5.2	The European Regulatory Framework (SES I/SES II and AVSEC) .....	29
5.2.1	Security Aspects of Regulation (EC) N° 1035/2011.....	30
5.2.1.1	Security Management Systems.....	30
5.2.1.2	Contingency Plans .....	30
5.2.1.3	Other Security Aspects.....	30
5.2.2	Security Aspects of Regulation (EC) N° 73/2010.....	31
5.2.3	Security Aspects of Regulation (EC) N° 300/2008 (not SES related) .....	32
5.3	The National Regulatory Framework .....	33
<b>6.</b>	<b>Governance and Organisation .....</b>	<b>34</b>
6.1	Governance.....	34
6.1.1	Roles and Responsibilities in Aviation Security .....	35
6.1.1.1	Global Level.....	35
6.1.1.2	European Level .....	35
6.1.1.3	National Level.....	36
6.1.2	Specific Roles and Responsibilities in ATM Security at National Level.....	36
6.1.3	Consultation.....	38
<b>7.</b>	<b>Oversight Programme.....</b>	<b>39</b>
	<b>ANNEX A – Acronyms .....</b>	<b>41</b>
	<b>ANNEX B – Definitions .....</b>	<b>43</b>
	<b>ANNEX C – Roles and Responsibilities in ATM Security.....</b>	<b>47</b>
	<b>ANNEX D – Generic Guidance for Oversight of ATM Security Management Systems .....</b>	<b>57</b>

QUESTIONNAIRE ON COST AND BENEFITS OF SECURITY (NSAS, ANSPS).....78

**4. EASA Standardisation Inspections & other activities.....129**

**ANNEX E – ATM Security Related Material Basic Documentation.....131**

## LIST OF FIGURES

<b>Figure 1: Resilience Umbrella .....</b>	<b>10</b>
<b>Figure 2: Cyber Security Context .....</b>	<b>11</b>
<b>Figure 3: Cyber Resilience Context.....</b>	<b>13</b>
<b>Figure 4: Malspace in Cyberspace .....</b>	<b>17</b>
<b>Figure 5: Cyber Governance and Partnering.....</b>	<b>17</b>
<b>Figure 6: Cyber Resilience Framework.....</b>	<b>18</b>
<b>Figure 7: Safety and Security Interface.....</b>	<b>24</b>
<b>Figure 8: Air Navigation Services .....</b>	<b>31</b>
<b>Figure 9: Separation of Regulatory, Oversight and Implementation Functions .....</b>	<b>39</b>
<b>Figure 10: Governance in Aviation Security.....</b>	<b>55</b>
<b>Figure 11: National ATM Security Organisation Chart .....</b>	<b>55</b>
<b>Figure 12: ATM Security Framework.....</b>	<b>58</b>
<b>Figure 13: Security Management Systems Overview .....</b>	<b>59</b>
<b>Figure 14: Generic Security Oversight Process.....</b>	<b>62</b>
<b>Figure 15: Organisation and Deployment of a Fictitious ANSP.....</b>	<b>125</b>



## LIST OF TABLES

<b>Table 1: Roles and Responsibilities in ATM Security .....</b>	<b>38</b>
<b>Table 2: Security Oversight Documentation Process.....</b>	<b>63</b>
<b>Table 3: ATM Security Oversight Authority .....</b>	<b>121</b>
<b>Table 4: Types of Monitoring Activities .....</b>	<b>122</b>
<b>Table 5: List of Auditors/Inspectors for ATM Security Oversight .....</b>	<b>124</b>
<b>Table 6: Schedule for Security Oversight of an Entity .....</b>	<b>126</b>



## EXECUTIVE SUMMARY

One year has passed since the version 1.0 of this Manual was published. In the meantime, ICAO has released the ATM Security Manual which has resulted in the alignment of parts of this document. At the same time, comments received from States have also been incorporated. This led to this updated version of the manual, version 2.0, which has been produced in support of national authorities responsible for ATM security oversight, namely the Appropriate Authorities (AA), in the context of ICAO, and the National Supervisory Authorities (NSA) in the context of the Single European Sky (SES).

Security oversight is a State responsibility and a fundamental function to improve the overall security process. It allows to verify compliance on the one side and, more important, to identify improvements towards a dynamic efficient security able to anticipate and mitigate main threats and risks to ATM. By guaranteeing security compliance, security oversight contributes to improving trust in the ATM system.

This manual is intended to support the national ATM security oversight function. The main customers of the manual are therefore the Appropriate Authorities (AA) and the National Supervisory Authorities (NSA). In the context of the SES, the NSA responsibilities regarding ATM security oversight are twofold:

- on the one side, they have to carry out the security inspections of ANSPs; and on the other hand;
- they are subject of EASA standardisation inspections, aimed at monitoring the application of relevant regulations and of their implementing rules by the national aviation authorities.

Nevertheless, NSAs are not the only final customer of this manual since ATM security goes beyond the remits of the Single European Sky (SES) regulatory framework. All national civil and military authorities responsible for aviation security and airspace security are addressed in the manual.

This manual provides guidance to the national authorities responsible for aviation and ATM security on:

- the understanding, context and scope of ATM security and its interfaces with the broader aviation security;
- how to carry out the oversight of ATM security management systems;
- how to be prepared for external ATM security oversight e.g. in the context of ICAO, ECAC and EASA audits or inspections.

## 1. INTRODUCTION

Security oversight is a fundamental function to improve the overall security process in a proactive manner. It is the responsibility of the State security authorities. It allows to verify compliance on the one side and, more important, to identify improvements towards a dynamic efficient security able to anticipate and mitigate main threats and risks to ATM. This aim is best achieved by introducing a holistic and systemic approach to security e.g. via the development and implementation of security managements systems.

By guaranteeing security compliance, security oversight contributes to improving trust in the ATM system.

It also facilitates security assurance and the validation process on the part of the organisations implementing the security requirements and helps improve the security loop Plan-Do-Check-Act, which thus enhances the quality of security management.

Training, accreditation and designation of Security Auditors are key aspects of ATM security performance. The quality of security oversight will depend on the quality of training for security auditors, thus impacting on the overall result of the national aviation security programme. Therefore, the quality (and quantity) of security auditors is a major aspect of national aviation security performance.

A national ATM Security Oversight Programme should not run in isolation but as an integral part of the broader National Aviation Security Programme.

## 2. AIM

This manual is intended to support the national ATM security oversight function in the European context and help States to better implementing their national security plans. The main customers of the manual are therefore the Appropriate Authorities (AA) in the context of ICAO and the National Supervisory Authorities (NSA) in the context of the Single European Sky (SES).

The NSA responsibilities regarding ATM security oversight are twofold:

- on the one side, they have to carry out the security inspections of ANSPs; and on the other hand;
- they are subject of EASA standardisation inspections (see chapter 6.1.1.2), aimed at monitoring the application of relevant regulations and of their implementing rules by the national aviation authorities. Since EASA competences have been extended to ANS/ATM (Regulation (EC) N° 1108/2009, see chapter 6.1.1.2) it means that EASA standardisation inspections will cover the requirements laid down in Commission Implementing Regulation (EU) N° 1035/2011; this includes **security** and **contingency** requirements. Eventually, ICAO would also include ATM security within its USAP (Universal Security Audit Programme).

This manual has been developed in support of **both** NSA obligations; inspect ANSPs security management systems and compliance against EASA standardisation inspections.

Nevertheless, NSAs are not the only final customer of this manual, since ATM security goes beyond the remits of the Single European Sky (SES) regulatory framework. All national civil and military authorities responsible for aviation security and airspace security are addressed in the manual. This is due to the scope and interfaces of ATM security within the overall umbrella of aviation security (see chapter 3).

The manual is also of interest to those organisations which are subject to security inspections by the national authorities; mainly the air navigation service providers (ANSP), but not exclusively, since others, like Aircraft Operators and Airport Operators also play a role in ATM security.

The manual provides an overview on the different aspects of ATM security, its interdependencies with other parts of aviation security and airspace security, the roles and responsibilities related to ATM security and its regulatory framework at global, European and national level.

The objective is to provide national authorities with a rationale of the different aspects around ATM security and its oversight function. This is done in a holistic approach, in the framework of the national responsibilities regarding aviation security as a whole. Therefore, the manual provides for the:

- WHAT: scope, what is ATM security and what are its interdependencies;
- WHY: the regulatory framework and national obligations;
- WHO: roles and responsibilities (Annex C);
- WHERE are we: self-assessment questionnaires (Annex D);
- HOW: security oversight process and questionnaires; high-level questionnaires and

detailed inspection questionnaires (Annex D);

- WHEN: oversight programme (Annex D).

The main body of the manual provides a rationale and a framework for ATM security oversight, and could be applicable to any State. The Annexes are meant to be customised according to the specificities of particular States. The annexes are living documents which must be updated regularly. They include a process template to support States to establish their own oversight plan. It also includes tables with points of contact detailing names, roles, specific responsibilities and contact information of all relevant parties.

The manual should be approved by the appropriate national security authority (normally the Appropriate Authority or the Civil Aviation Authority – CAA) and properly disseminated to all parties involved. Once completed, annexes C and D should be classified as Restricted and be subject to applicable national protective measures.

### 3. SCOPE

The scope of this manual is the oversight of ATM security at national level. FAB and Network (Network Manager – NM) dimensions are not fully addressed within the scope of this document. However, initial requirements for FABs are tabled in Annex D.

It must be emphasised that the scope of this manual is broader than the security requirements laid down in the SES regulatory framework e.g. Commission Implementing Regulation (EU) N° 1035/2011. This regulatory framework, although relevant, is limited and does not cover the full scope of ATM security as described hereafter. Therefore, the scope of this manual goes beyond the SES regulatory framework and covers the full spectrum of ATM security aspects.

ATM security must not be addressed in isolation but as an integral part of the overall aviation security system following a holistic approach. A national ATM security oversight programme should consider all aspects relevant to ATM security including possible interfaces with other aviation security related areas. A common understanding of what is ATM security, in the framework of the broader concept of aviation security, is therefore needed.

#### 3.1 Holistic Approach

One of the main conclusions of the Aviation Security Workshop held on 11 June 2010 in Berlin was a need for a 'holistic view' covering the variety of threats and challenges to aviation security (*the weakest link in the chain is the one likely to break*):

- for all phases of air transport;
- on the ground and in the air;
- considering all operational processes related to the Airport , the Aircraft and Air Traffic Management;
  - this includes passengers, staff, baggage, cargo, supplies, catering, check-in, border control, security screening, traffic management, fuelling, etc.
- having passenger awareness of its part in the process;
- global view: importance of international relations and the need for working with/through wider regional/international organisations such as ECAC/ICAO/EUROCONTROL/TSA as well as with industry stakeholders;
- Need to improve resilience of the whole air transport system;
- Need for a conceptual approach: to move from being 'reactive' to becoming 'anticipative';
- Need to better define current and future vulnerabilities.

Security requires a holistic approach. Interfaces between aviation security components deserve special attention e.g. ATM security, CNS security (ADS-B, GNSS, data links,...), Airspace Security and Airport Security. ATM security must be embedded as an integral part of the aviation security system and therefore it should be included in the National Aviation Security (AVSEC) Programme.

In this holistic scenario, security must be understood in a broad sense, gate-to-gate, and in a comprehensive manner, addressing all types of threats and including all interested parties and stakeholders.

Comprehensive national ATM Security must be developed in close cooperation with all relevant actors concerned: civil and military regulators and authorities, ANSPs, Airspace Users (Aircraft Operators, General Aviation and Military), Manufacturer Industry and Research Centres. Security actors also include, at international level, all institutions concerned: EC, ECAC, ICAO, EASA, SJU, States, FABs and Network Manager.

### **3.2 Understanding Aviation Security (AVSEC)**

When dealing with the different aspects of Aviation Security (AVSEC) a variety of names is often mentioned in different publications and, in many cases, definitions are missing. It is very important for the sake of clarity that all stakeholders in AVSEC have a common understanding and share the same definitions to address the different components within the overall AVSEC framework.

Currently agreed and used definitions related to aviation, ATM and Airspace Security are provided in Annex B.

Linked to the definitions is the discussion about the different aspects included in the overall term AVSEC.

The NEASCOG (NATO EUROCONTROL ATM Security Coordinating Group) ATM Security Threat and Risk Assessment identify several threat scenarios:

- Airborne threats:
  - Terrorist acts:
    - 9/11 situation: Renegade<sup>1</sup>; Commercial/General Aviation, private jets, low speed aircraft
    - Conventional hijack
    - Bomb on board
    - MANPADS
    - Improvised UAV/cruise missile
    - Other, in accordance with intelligence input
  - Illegal acts:
    - Airspace violation/intrusion i.e. for criminal activity
    - Unruly passenger
    - Laser illumination
- Attacks against infrastructure:
  - Airports e.g. terminals as crowded places and air side
  - ATM/CNS facilities and means

---

<sup>1</sup> A situation where a civil aircraft is used as a weapon to perpetrate a terrorist attack is usually referred to as a RENEGADE (NATO)



- Control centres
- Cyber attacks (information systems):
  - Data processing systems
  - Databases
  - Information management networks
- Electromagnetic attacks:
  - Jamming
  - Interference
  - Spoofing of CNS systems

An ATM security system must address the full spectrum of threats to aviation and therefore take due account of all different aspects within the common umbrella *Aviation Security*.

### **3.2.1 AVSEC Protection Layers**

Security measures are much more efficient when they follow a layered approach. To cope with the threats listed above a number of AVSEC layers should be implemented in a consistent and coordinated manner.

The following aspects should be considered as AVSEC components:

- Intelligence Support
- Threat, Risk and Vulnerability Assessments
- Personnel Security
- Security Information Sharing
- Crisis management
- Airport Security
  - Physical Security; access control and searching
  - Aircraft Security (on the ground)
  - Anti-MANPADS measures (patrolling, surveillance)
  - INFOSEC (cyber defence)
  - Laser illumination
- ATM Security (Self-Protection)
  - Physical Security
  - INFOSEC

- ATM Security (Collaborative Support); contribution of the ATM system to civil aviation security, national security and defence, and law enforcement
  - Support to aviation security
    - Support safeguarding civil aviation against unlawful interferences e.g. hijack, MANPADS and laser attacks
  - Support to national security and defence
    - Assist military air defence operations
    - Protect airspace during major events e.g. through airspace design
    - Protect special flights e.g. political leaders, VIP flights, flights subject to diplomatic clearance etc.
    - Support emergency response and crisis management
  - Support to law enforcement
    - Support law enforcement air operations against domestic and cross-border crimes
- Airspace Security
  - Early Threat detection of Possible Suspicious Flights
    - Positive Flight Identification: Flight Plan Security screening, Pilot/aircrew positive identification, Airframe positive identification
    - Third countries air carriers security issues e.g. air cargo security
    - General Aviation issues
  - Airspace Security Incident Management (ASSIM)
    - Aircraft Security (in-flight security measures)
    - Airspace Security Incidents (hijack, bomb on board, COMLOSS, improvise UAS/missile)
    - RENEGADE (Airspace Security Incidents declared as such by the appropriate authority)
- CNS Systems Security
  - Physical Security
  - COMSEC (Electronic Counter Measures)
  - INFOSEC (cyber defence)
- Additional
  - Security culture, education, awareness, training and exercises
  - Assurance, assessment, oversight, audits, monitoring
  - R&D
  - Regulations (national and international)
  - Industrial activities and developments

### 3.3 Understanding ATM Security

ATM Security is major component of Aviation Security (AVSEC). ATM security differs from AVSEC in the sense that ATM security has dual requirements of protection of the ATM system against threats and vulnerabilities and the provision of ATM security services in support of organizations and authorities engaged in aviation security, national security, defence, and law enforcement. ATM security is concerned with those threats that are aimed at the ATM System directly such as attacks on ATM assets, or where ATM plays a key role in the prevention of or response to threats aimed at other parts of the aviation system (including national and international high-value assets) and in limiting the effects of such threats on the overall ATM Network.

It comprises two key areas:

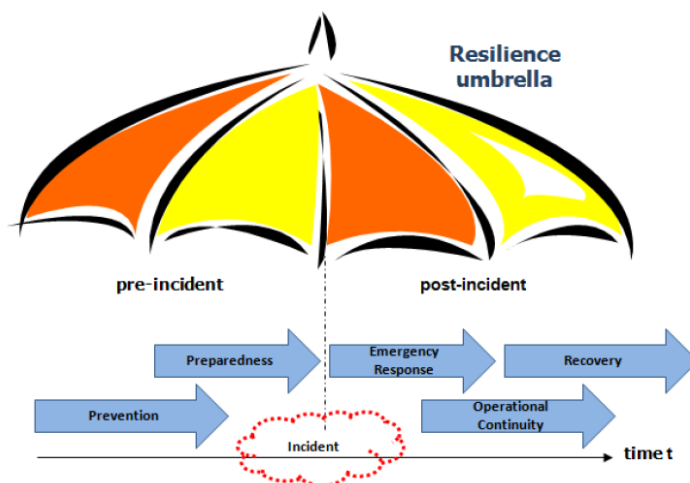
- **Self-protection of the ATM system:** this addresses security and resilience of physical infrastructure, personnel, information and communication systems, ATM/CNS infrastructure and networks;
- **ATM Collaborative Support** to aviation security, civil and military authorities responsible for national security and defence and law enforcement.

ATM Security has an interface with Airspace Security revolving around national security and defence requirements, operational aspects of collaborative support, and technological security and interoperability between civil and military systems.

Security threats may be directed at aircraft or through them to targets on the ground. The ATM facilities and systems may also become threat targets. Although ATM cannot by itself address all issues, it nevertheless has to provide responsible authorities with the requested help in all phases of the security occurrence in accordance with national, ICAO and other relevant international rules. The international dimension imposes the uniform and effective application of suitable measures.

ATM has to support national security in respect of the identification of flights entering a State's national territory, and Air Defence organisations have to be provided with all ATM information relevant to their task.

On the other hand, particular attention will need to be paid to the preparation of contingency plans designed to handle degradations of the ATM system and security-related emergency situations. Indeed, contingency planning is an essential part of the overall security cycle. It aims at getting the system back to 'normal' as soon as possible after an attack. This will prevent the attackers/terrorists to exploit 'twice' the success of an attack; hitting an ATM target and disrupting normal operations for a long period due to overreaction and lack of contingency plans. The associated economic impact of lack of contingency must also be considered. The figure below illustrates a complete resilience cycle including contingency planning:



**Figure 1: Resilience Umbrella**

### 3.4 The Transversal Security Measures

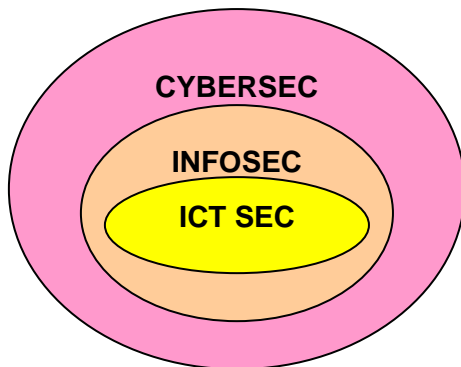
In general terms, security measures range across a number of security disciplines. It does not matter if the asset to protect is an aircraft, an airport, a control centre or an information network, all security elements apply at a certain degree:

- Intelligence support: security without intelligence is meaningless; intelligence support is a transverse requirement for threat assessments, threat watch and security alert levels declaration;
- Security information exchange between national authorities, security and intelligence organisations and ATM security managers. It should include security warnings, threat and alert levels, incident identification and notification (i.e. security breaches), reporting and incident resolution follow-up;
- Physical security: access control, perimeter protection, screening, control checks;
- Personnel security: vetting, security clearances, recruitment policy, staff regulations;
- Information security: protection of information; confidentiality, availability, integrity (CIA).

### 3.5 Cyber Security

The cyber threat will most likely be one of the main security issues in aviation and the Single European Sky. The ATM system will massively migrate to an IP (Internet Protocol) based infrastructure and operate in accordance with the network centric operations concept, where real-time information sharing is key. The complexity and criticality of information security and its governance demand that it be elevated to the highest organisational level. As a critical resource, information must be treated like any other asset essential to the survival and success of the ATM system.

Cyber security is a concept born in 1994 which embraces traditional INFOSEC and ICT disciplines. It requires a multidisciplinary approach and should be at the core of the ATM security management. The performance of the Single European Sky will broadly depend on its resilience to guarantee uninterrupted service, and SES resilience will mainly mean cyber resilience. The aviation intranet will not be an ICT system but a net-centric system which falls under the cyber security domain (the so called 5<sup>th</sup> warfare domain in the military environment).



**Figure 2: Cyber Security Context**

### 3.5.1 Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is about ensuring that services vital to the society continue to function. Critical infrastructures are assets, systems, services, networks, etc., that provide vital services that are key to society and which disruption could have severe security and economic consequences. The interdependencies of critical infrastructures mean that many sectors, such as air traffic, can be affected by a threat to a single critical infrastructure, such as the European aviation network.

The European aviation network should qualify as critical infrastructure for Europe and therefore its security requirements could be covered (at least partially) by Council Directive N° 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The aviation network will become an extremely attractive target for cyber attacks (not necessarily carried out by terrorists or individual hackers exclusively but also other sources e.g. competitor States sponsoring cyber attacks, hidden behind the difficulty of attribution of a cyber attack). Attackers can get extremely robust capabilities at a considerably low cost.

In this context, appropriate levels of security are crucial to ensure real-time information exchange guaranteeing confidentiality, integrity and availability (CIA) of ATM data. The aviation intranet and its information exchange requirements demand a robust security policy and security solutions to enable and protect the expected SES performance.

### 3.5.2 The Cyber Threat

Information is an asset to the aviation organisations which needs to be protected. These organizations may have a great deal of information about employees, passengers, flight crews, flight operations, historical records, and financial status. Should this confidential information fall into the hands of an unauthorised entity, this breach of security could lead to ATM system shutdown, unlawful interference with aircraft flight operations, lawsuits, or loss of life. Protecting confidential information is, therefore, a prime ATM security requirement and, in many cases, an ethical and legal requirement.

ICT security refers to the application of security controls to protect ATM ICT systems against the degradation of confidentiality, integrity, and availability (CIA) from intentional or accidental causes. The ATM ICT system security applies to people, procedures, data, software, and hardware that are used to gather and analyse digital and analogue information used in ATM.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection (CIIP); COM(2011) 163 final states that *“new and technologically more sophisticated threats have emerged. Their global geopolitical dimension is becoming progressively clearer. We are witnessing a trend towards using ICT for political, economic and military predominance, including through offensive capabilities. ‘Cyber-warfare’ or ‘cyber-terrorism’ are sometimes mentioned in this context”*.

***“It is the great irony of our Information Age – the very technologies that empower us to create and build also empower those who would disrupt and destroy”<sup>2</sup>***

In order to gain a more comprehensive understanding of cyber threats, it can be useful to review and align some terminology for the purpose of this manual.

#### 3.5.2.1 Concepts

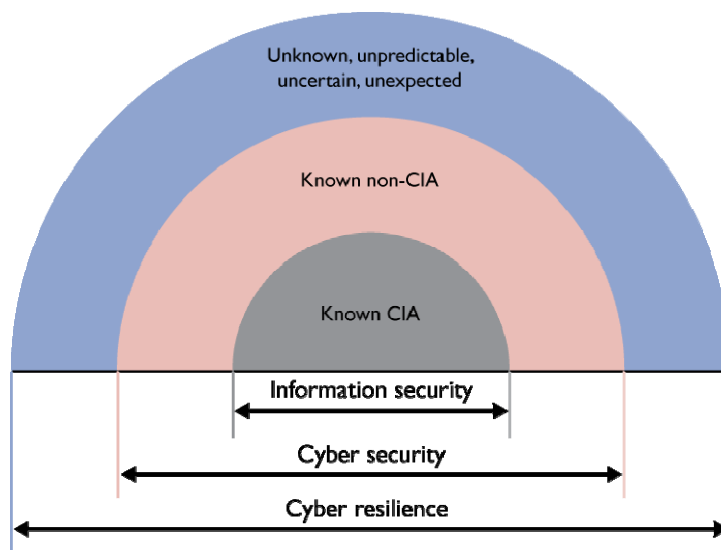
- **Cyberspace** is the always-on, technologically interconnected world; it consists of people, organisations, information and technology. As much as cyberspace offers enormous possibilities to its legitimate users, it provokes an equal level of risks. Cyberspace is very dynamic and is constantly changing in unpredictable ways. As a result, it might de-risk criminal activities and facilitates collaboration between criminals.
- **Cyber Security** is an organisation's ability to secure its people, information, systems and reputation in cyberspace. Cyber security assists in understanding the scope of cyberspace and the potentials threats. Dealing also with threats that may be outside the organisation, contributing to the public good and at the same time to the organisation's own security by improving the security of others.

---

<sup>2</sup> US President Barack Obama

- **Malspace:** All benefits that cyberspace offers to organisations (i.e. collaboration, innovation, faster development of new technologies, global connectivity) are also available to attackers. This entire malicious industry, with unprecedented collaboration and a complete marketplace for buying and selling hacker tools could be considered as malspace.
- **Cyber attack** is an offensive activity executed in malspace and which was designed and performed to deny, degrade, disrupt, manipulate or destroy information or ICT systems.
- **Hactivism** is cyber-enabled social activism. Like traditional activism, hacktivist activities range from peaceful protest to highly damaging criminal activity.
- **Cyber Resilience** is the organisation's capability to withstand negative impact due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace. It requires an adapted cyber security framework and above all regular updated risk and incident management systems which consider also the threats "we don't know we don't know" on top of those "we know we know" and those "we know we don't know".

Relative position:



**Figure 3: Cyber Resilience Context**

### 3.5.2.2 Threat Classification

Many threats from cyberspace are to the Confidentiality, Integrity and Availability (CIA) of information and systems – the traditional remit of the Information Security function. Likewise, Information Security fundamentals, including controls, standards and governance go a long way to addressing threats from cyberspace and will continue to do so in the future. Those can be grouped along the following categories:

- **Exploitation** purposes such as "advanced persistent threats" (i.e. continuous and coordinated attacks against government agencies and the public sector) for economic

and political espionage purposes, identity theft, the recent attacks against the Emissions Trading System or against government IT systems (i.e. the recent attacks against the French Government);

- **Disruption** purposes such as Distributed Denial of Service attacks or spamming generated via botnets (e.g. the Conficker network of 7 million machines and the Spanish-based Mariposa network of 12,7 million machines), Stuxnet and cut-off of communication means;
- **Destruction** purposes. This is a scenario that has not yet materialised but given the increasing pervasiveness of ICT in Critical Infrastructures (e.g. smart grids and water systems), it cannot be ruled out for the years to come (World Economic Forum, Global Risks 2011).

However, in order to be secure in cyberspace, organisations must address additional threats far beyond the boundaries of the CIA triad:

- **Non-CIA threats:** examples are hacktivism attacks on organisations' reputation, unintended consequences from legitimate information release and unintended impact from the use of cyberspace.
- **Threats to CIA and systems in cyberspace are magnified.** This magnification can give publicity literally on a world-wide scale. Examples are the impact of hacktivist actions from Wikileaks, Anonymous and Lulzsec.
- **World-wide scale of crime in cyberspace**, because cyberspace:
  - De-risks criminal activity for the perpetrators;
  - Provides powerful weapons;
  - Concentrates the targets in one place: the internet;
  - Obscures the perpetrators' location.

### 3.5.2.3 Threat Agents

Threats agents may vary from:

- Lone operatives: individual hackers with different motivation (the challenge to overcome cyber defences, cause an accident, bring the attention of the authorities, raise a political, social or personal issue, blackmail, sabotage, simply highlight the vulnerability of the system, mentally ill, etc.);
- Organised groups:
  - Terrorists;
  - Criminals;
  - Protesters, activists (hacktivists), etc.
- Third party organisations or even competitor States sponsoring cyber attacks.

The abovementioned threat agents are mostly, if not always, the executioners of the threat itself. Since cyberspace became more and more active and as a result became more interesting for organised crime (in whatever form), another group of threat agents became very active:



- The Cyber Crime Marketplace with formal and informal e-biz sites, private collaboration spaces, hosted market sites;
- Currency and Settlement Services;
- Industry groups for Reconnaissance and vulnerability scanning services, extraction and laundering services, planning and coordination services, malware development services, fraud services, etc.

In all cases, major consideration should be given to the *inside threat*. 'Insiders' i.e. disaffected or manipulated staff pose a major risk since they might be familiar with the security processes and vulnerabilities of the organisation.

Another important consideration in cyber security is the difficulty (if not the impossibility) to attribute an attack. *Hidden* behind this difficulty of attribution of a cyber attack, some States are suspicious of having launched or sponsored cyber attacks against the US and some European States. This phenomenon is introducing a paradigm change in the geo-strategic scene; it has already been mentioned that cyber security is the 5<sup>th</sup> warfare domain. As part of the future new 'cyber strategy' of the Pentagon, the US could classify serious cyber attacks as 'acts of war' or hostile acts. Response to such cyber attacks might include the use of conventional weapons.

#### 3.5.2.4 Threat Assessment

The 3 pillars of information security are:

- **Availability** (reliable information must be at the disposal of legitimate users when needed);
- **Integrity** (the information provided to the legitimate user is the correct expected one) and;
- **Confidentiality** (only authorised legitimate users get access to the appropriate information, on a 'need to know' or 'need to share' basis).

Notorious threats against these 3 pillars are:

- **Denial of Service** (availability part of security): disruption of access to or use of one or more critical components of the ATM infrastructure (data and voice - ground/ground and air/ground);
- **Data Tampering** (integrity part of security): take control of a system (i.e. import false data, unauthorised modification or destruction);
- **Unauthorised disclosure/access** (confidentiality part of security): it is true that more and more information related to ATM is made public. However, some flights remain sensitive and related data should remain restricted.

Regarding the IP migration part, it should be noted that in the future aviation intranet, public vs. private infrastructure will be more relevant. It is certain that internet access will be more and more used and this will highly increase the risk.

Examples of typical cyber attacks are:

- **Data Tampering**

In cyber space, the use of Trojan Horses is one of the ways used by perpetrators to take control of computer systems. The Trojan Horse penetrates a system through for instance an

email or "recently" installed software and tries to look for unprotected "backdoors" in the system. The backdoors might be used at a later stage, even months or years later to compromise a system. The collection of compromised systems is referred to as a Botnet<sup>3</sup>.

- **Network Infrastructure Attack**

The best known example is the "Stuxnet"<sup>4</sup> attack, which purpose was to sabotage specific Siemens hardware. This hardware is extensively used in industrial plants. Stuxnet became notorious when a nuclear installation in Iran was under attack.

- **Application Attack**

A well-known and, at the same time notorious application, Attack will try to exploit Structure Query Language (SQL) vulnerabilities, called SQL Injections. It is used to attack the security of a public web site by inputting specific SQL statements in unprotected web forms and as a result databases can be altered. SQL Injection Attacks are considered one of the top 10 web application vulnerabilities.

- **Reconnaissance Attack**

This type of attack tries to gain information about (a) potential victim(s) that will help implement a future attack.

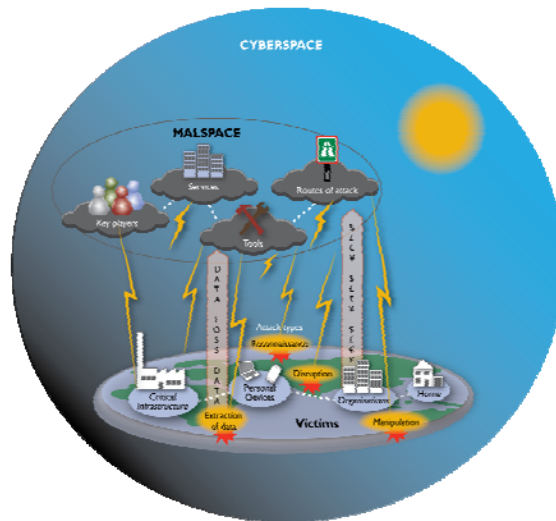
- **Disruption, Extraction and Manipulation Attack**

These attacks try to disrupt a business, system or service or try to extract or manipulate data from victims.

---

<sup>3</sup> A **botnet** is a collection of compromised systems or computers connected to a network i.e. the Internet (these are also known as 'bots'). When a computer becomes compromised it becomes a part of a botnet.

<sup>4</sup> **Stuxnet** is a **computer worm** (a self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes/computers on the network, and it may do so without any user intervention) discovered in June 2010. It initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment. The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes.



**Figure 4: Malspace in Cyberspace**

### 3.5.2.5 Building Cyber Resilience

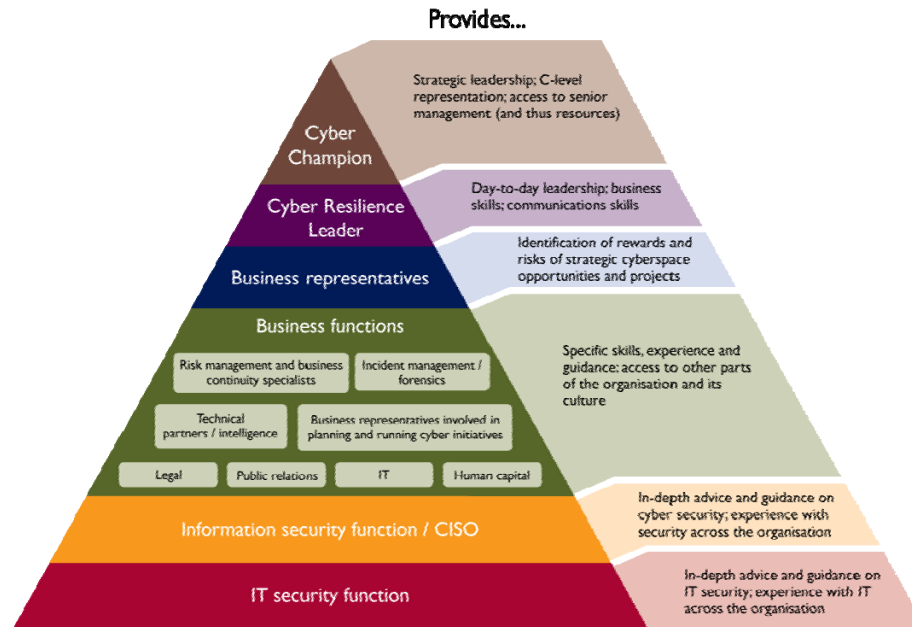
Cyber Resilience requires recognition that organisations must prepare now to deal with severe impact from cyber threats than can or cannot be predicted or prevented. Without going into detail, cyber resilience is implemented through:

- Reviews and assessments on a regular basis of the Information Security controls like the “SANS 20 Critical (Cyber) Security Controls” or the “35 steps to protect yourself from Cyber Espionage” suggested by the Australian Defence Signals Directorate (ADSD);
- Adopting a solid Cyber Resilience Framework will enable an organisation to respond more effectively and consistently to the challenges of threatening cyberspace activities and to be more resilient in cyberspace. A possible framework should contain at least the following elements:



**Figure 5: Cyber Governance and Partnering**

- One of the key success factors of a Cyber Resilience Framework is the solid composition of the Cyber Resilience Group, responsible for Cyber Resilience Governance within and throughout the organisation.



**Figure 6: Cyber Resilience Framework**

- Cyber Resilience Information Sharing with other organisations is crucial and of vital importance. Criminal organisations collaborate and so should the legitimate world. A common taxonomy of operational Cyber Security Risks, which is structured around a hierarchy of classes and sub classes, is mandatory for a well functioning exchange process of information.

### 3.5.2.6 Specific Key Findings Regarding Cyber Security and Cyber Resilience

- The benefits from cyberspace are immense and so are the risks;
- Trust is a most elusive notion: the internet was built on trust, and that is why it is so vulnerable;
- Organisations must embrace uncertainty and develop cyber resilience;
- New technologies will generate new vulnerabilities;
- Malspace is a global industry that has evolved to deliver cyber attacks;
- Hactivism presents significant threats to an organisation, not just Information Security;
- The spectrum of malicious actors is expanding;
- Cyber Security is more than Information Security;
- Cyberspace has vastly increased the Information Security Risks;
- Information Security is and stays fundamental and becomes even more important in cyberspace;

- It is essential to collaborate with other organisations to share intelligence gathering and good practices;
- Cyber Resilience requires an evolving solution to meet the ever moving threats;
- Cyber Security is not trivial and we must stop acting like it is;
- In addition to technology controls, we must also ensure effective controls for people, facilities, management and operations;
- Cyber threats cannot be addressed in isolation.

## 4. POLICY AND STRATEGIC PLANNING

The policy sets the basic principles for ATM security which forms the basis for security developments e.g. Security Management Systems (SeMS), and guide security authorities and managers across all the security process: Regulation/Implementation/Oversight. The policy is the driver of security activities whilst the strategic objectives set up the goals of the organisation in security.

### 4.1 Mission

The national ATM security system mission is:

- Improve resilience of the ATM system to safeguard civil air transport from threats and vulnerabilities that might cause any disruption to civil aviation;
- Contribute and provide the necessary support to aviation security and national civil and military authorities responsible for security, defence and law enforcement.

### 4.2 Vision

*The national ATM security system must be trusted by the national government, the general public, the FAB peer countries and the Network Manager that it is secure, resilient and well-protected from any unlawful activities that could potentially cause disruption to civil air transport.*

Security is primarily a State responsibility. However, its international dimension imposes the need for harmonisation. In the framework of the SES, the FAB and Pan-European network dimension must be fully addressed.

The key aspect in a multinational/multi stakeholder environment is **trust**. The creation of a mutual trust framework is a paramount requirement. In this regard, clear and robust governance is a fundamental need.

### 4.3 Strategic Objectives

- Protect citizens, territory, airspace, critical infrastructure and interests from threats against the air transport system;
- Ensure safety and security at the maximum extent possible whilst complying with international and national associated legal frameworks;
- Provide the national ATM with a relevant role in the resilience of the overall transport supply chain;
- Establish standard, efficient and certified oversight mechanisms;
- Adequate awareness, training and licensing of all relevant staff;
- Facilitate and enhance cooperation among all parties involved;
- Elevate security culture and awareness at the level of safety culture;
- Implementation-oriented: main target/deliverable is the implementation of a harmonised, seamless, robust Security System, overcoming national (and regional) fragmentation;

- Support uninterrupted ATM operations; security is not only a societal demand but also an enabler to guarantee that expected levels of safety, capacity and cost-effectiveness are met.

#### **4.4 ATM Security Principles**

- a. Security must be commensurate with the risks;
- b. Consider all aspects/scenarios (holistic view);
- c. Be effective;
- d. Be practicable;
- e. Be sustainable;
- f. Intelligence-led, threat-based and risk-managed;
- g. Multi-layered, proportionate response;
- h. No overrule: make use of best practices and standards at the maximum possible extent (not more security but better security);
- i. Single regulator: CAA;
- j. Partnership (PPP: Public Private Partnership); industry involvement;
- k. Proactive and systematic approach;
- l. Holistic approach; all security components are interrelated. ATM security should be developed in line with other aviation security components;
- m. Global view; overlapping *internal* and *external* security; regional cooperation (FAB), network dimension (EU Network Manager).

#### **4.5 Fragmentation Analysis**

The main obstacle to progress a national harmonised security system might be fragmentation.

Fundamental input for national authorities is a fragmentation analysis report highlighting:

- Implementation status;
- Gap analysis.

The results will help identify areas of concern and future work.

Possible fragmentation at both national and regional levels can be assessed through questionnaires and surveys (and through the annual SES reporting template). Overcoming possible fragmentation is a must for the realisation of a robust national aviation security programme. Moreover, it will enable reaching harmonised security baselines at both FAB and Network levels. Security self-assessment questionnaires are provided in Annex D.

#### **4.6 Education, Awareness and Training**

Education, awareness and training (including simulations and exercises) requirements are essential in the framework of ATM security. Indeed it is a fundamental enabler of the trust framework.

Like for Safety, Security requires sound and mutually recognised security professionals in all areas of concern: physical, personnel, organisational and technical security; Cyber security; airspace security; CNS security; risk and threat assessments; education, awareness and training; oversight and monitoring, etc.

Training the trainer is a first step. Designated training centres and training staff, security job profiles, accreditations, mutual recognitions, training categories and diplomas, recurrent training, revalidation tests are all part of the requirements. The same holds true for exercises; simulations, on line, live, video gaming type, etc.

Training, accreditation and designation of Security Auditors are key aspects of the ATM security performance.

The final goal of security education, awareness and training is to create and permanently enhance a consolidated **security culture**, fully integrated with the safety culture.



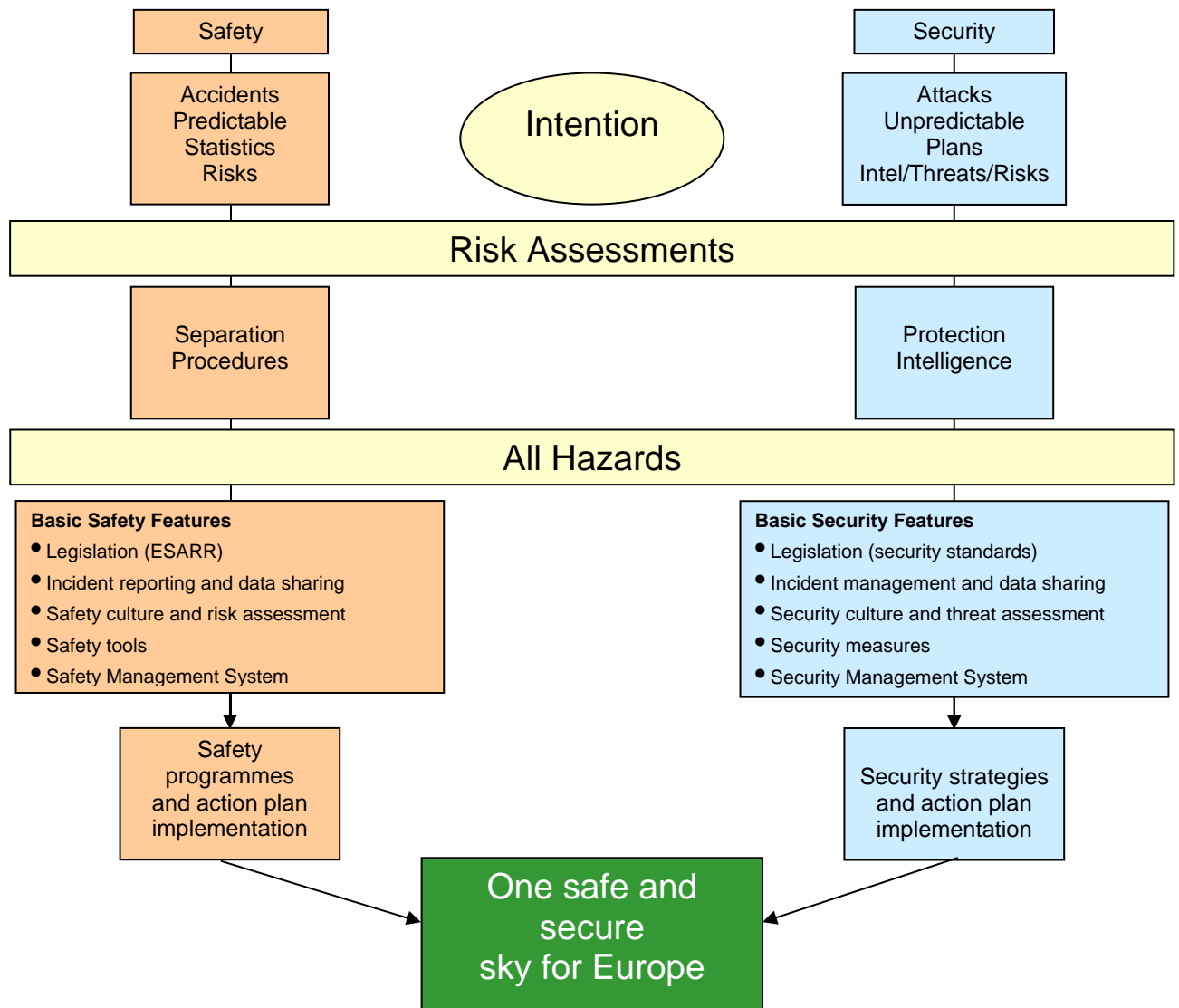
## 4.7 Safety/Security Interface

There is ongoing interest in analysing how safety and security interrelate with each other, and where synergies and savings can be achieved by a better interfacing both. Some analysts declare that safety and security merge as security and defence do. This might be true, especially in an IP-based net-centric operational environment such as SWIM<sup>5</sup>. In such an environment security is paramount. It will normally require more stringent requirements than safety. CIA (Confidentiality, Integrity, and Availability) INFOSEC requirements versus an intentional threat like cyber terrorists or state sponsored cyber attack need to be very robust compared to the same requirements versus unintentional incidents. This means that, in general, by meeting the security requirements, the safety requirements should by default also be met by far. Indeed in a network environment, the term referred to is security rather than safety (no reference exists to information safety but rather to information security). State authorities must look into the safety impact of security measures before they are implemented. In a similar way, safety implementations might have an impact on security. In this regard, the integration of safety and security (and maybe others like quality) management systems seems to be good practice, which is even referenced in the SES legislation (Commission Implementing regulation (EU) N° 1035/2011 laying down common requirements for the provision of air navigation services)<sup>6</sup>.

---

<sup>5</sup> SWIM: System Wide Information Management

<sup>6</sup> The safety, quality and security management systems may be designed and operated as an integrated management system



**Figure 7: Safety and Security Interface**

#### 4.8 Threat and Risk Assessment

In the framework of the SES, the main threat *will* be the cyber threat. This is because all ATM processes will migrate to cyber space (SWIM) and will become a target for cyber attackers.

Other emerging threats have to do with the operational introduction of new concepts (e.g. 4-D trajectory) and technologies in the CNS domain: ADS-B, GPS, new communications (datalinks). Spoofing, interference, jamming and unlawful exploitation of signals are the associated threats.

The operational introduction of Unmanned Aerial Systems (UAS) will also bring some risks. Security requirements must be an integral part, embedded by design, from the very start of any plan for UAS operations.

The rest of the classical threats (hijack, RENEGADE, bomb on board, physical attacks to infrastructure) will remain, but most probably mitigated due to implementation of security measures.

Third countries security (flights coming from 'insecure' areas) will require new measures to prevent e.g. air cargo security threats.

Security threat and risk assessments are the basis for further security developments. All issues mentioned above require a regular threat and risk assessment and follow-up. This will help identify new and emerging threats and threat evolution, providing for a continuous threat watch.

Providing for this capability (risk and threat assessment studies and methodologies) is a strategic area of development for ATM security.

ATM security threat and risk assessments are the **starting point** for security oversight. The outcome of the threat and risk assessment will facilitate the identification of:

- Focus areas where the provision/implementation organisations should look at when developing SeMS, and possible new or reviewed regulations could bring added value;
- Security objectives for ATM security. They must be realistic, clear, measurable, agreed and known by all players;
- Improvements to the Plan-Do-Check-Act security cycle;
- Finally, all elements above can be consolidated in a list of security **requirements** which are fundamental in the oversight process since **compliance** is checked against these requirements.

Security requirements stem from:

- Threat and risk assessments;
- National legislation;
- International legislation;
- International treaties.

All security requirements applicable to aviation (including ATM) should be laid down in specific national aviation legislation. This will enhance harmonisation and common understanding and will facilitate the oversight function.

National ATM security authorities must carry out a comprehensive threat and risk assessment. This can not be done in isolation but should be carried out in the context of the **national security environment**. The background for such assessment is:

- National security framework and threat assessments: they address the overall security environment and are applicable to all people, departments and institutions, public and private;
- National aviation security threat and risk assessment: should be an outcome of the National Aviation Security Committee (see Annex C). It is done in the context of the above national assessment;
- ATM security threat and risk assessment: is a part of the above assessment. Nevertheless, the ATM security authorities can go deeper in detailing the specific threats to ATM;

- Local threat and risk assessments: these are carried out by ANSPs, Airport Operators, Aircraft Operators and Entities to address specific issues and local security conditions. These threat assessments are part of the security management (e.g. SeMS) of the organisations and an integral part of the national aviation security programme.

When carrying out security threat and risk assessments, State authorities should consider input provided by international organisations e.g. ICAO, ECAC, EC, NATO and EUROCONTROL.

#### 4.9 Cost and Benefits of Security

Security is a State responsibility and a societal need. Nevertheless, it has traditionally borne challenges for public acceptance: it is costly, uncomfortable for citizens, never 100% efficient and too reactive. Like for safety, the benefits of security should be spelled out and made known to people and authorities. It should follow a ROSI (Return On Security Investment) model by which authorities and managers can duly justify that security investments are part of the business plan, providing added value (value for money) to the organisation.

Some examples of expected benefits from security are: increased awareness, better asset control (i.e. less theft, less misuse of ICT systems), better incident management i.e. increased reporting of abnormal situations and cooperation from all staff (security, as safety, is everybody's responsibility and part of corporate business), contributes to staff management (i.e. absence control, improved access control; visitors, suppliers). Without any doubt, a more secure environment improves working conditions. Synergies with safety and facility managers are also a benefit and a cost savings factor.

Security cases should be carried out in support of the business case when developing and implementing new regulations, processes, concepts or technologies. Like for safety this should be embedded into the standard business plans. One of the major outcomes expected from SESAR is a security case methodology and guidance.

On the other hand, appropriate funding for security is part of the regulatory framework.

The ICAO Aviation Security Manual states that: *'given that the establishment of a comprehensive **security oversight system** is essential if a State is to ensure the effective implementation of its national aviation security requirements and Annex 17 SARPs, the appropriate authority and other relevant authorities responsible for security oversight **should be provided with the necessary resources, both human and financial**, to be able to effectively carry out security oversight obligations on behalf of the State. It is essential that, because of anticipated or actual costs, States do not default on their responsibility for ensuring implementation of the NCASP (National Civil Aviation Security Programme) and all related Annex 17 SARPs, as well as implementation of security-related SARPs in other Annexes to the Convention on International Civil Aviation'*.

Furthermore, the Commission Implementing Regulation (EU) N° 1035/2011 on common requirements for the provision of air navigation services includes reporting requirement for ANSPs. As part of the annual plan, the ANSPs shall include *information on the implementation of **new infrastructure or other developments** and a statement how they will contribute to improving the level and quality of services*. It is clear that security investments, both in infrastructure and recruitment, must be **part of the annual reporting to the NSAs** and therefore information on the cost associated to security must be known to the authorities.

A questionnaire on cost and benefits of security is provided in Annex D.

#### 4.10 Crisis Management

An ATM Security system must support uninterrupted ATM operations; security is not only a societal demand but also an enabler to guarantee that expected levels of safety, capacity, environment and cost-effectiveness are delivered and any disruption mitigated in the shortest timeframe. A fundamental part of the ATM security system capabilities is related to the ability to the *respond and recover*. This will enable continuity of operations, even in a degraded mode for a certain period. National ATM must be able to assist the national crisis management authorities to plan, prevent, prepare, respond and recover the aviation system against security related crises, thus minimising impact on the transport network and accelerating full recovery time. This can be better achieved through the involvement and regular participation of ATM security experts in the activities of the appropriate national crisis management organisation.

#### 4.11 International Collaboration, Civil-Military Coordination

A national ATM security system should not be developed in isolation but in full consideration of the international (FAB and European Aviation Network) and global framework. It must take due account of other activities and developments at global scale and promote institutional cooperation and information sharing.

The civil-military dimension in security is an important aspect; and particularly relevant in the context of cyber and CNS security. Recently, ICAO has launched a strategic campaign to improve civil-military cooperation at a global level. ATM security has been identified as one of the main areas of work. At the same time, ICAO has developed an ATM Security Guidance document as a complement of its Aviation Security Manual to support States implementing the SARPs laid down in Annex 17 (Security) to the Chicago Convention.

Within the context of cooperation with other regions, the EU Neighbourhood Transport Plan responds to one of the EU's most ambitious policies; the development of closer relations between the European Union and its neighbours to the East and South. However, missing links in infrastructure, lack of security and safety hamper transport flows.

In the sector of aviation, the plan aims at the creation of a wider European Common Aviation Area (ECAA). The proposed actions are:

- Comprehensive air services agreements (ASA);
- Assist in the modernisation of ATM systems;
- Assist in achieving EU and international levels of aviation safety and security;
- Integrate neighbours into the Single European Sky.

## 5. REGULATORY FRAMEWORK

The national ATM security oversight programme must look at the full range of security regulations at national and international level, relevant to the provision of air navigation services, in order to provide for a consistent and comprehensive security oversight function. ATM security auditors must be familiar with regulations in place and under development, as well as with ongoing ATM security activities at national, regional and global level.

### 5.1 The Global Regulatory Framework

Aviation Security is one of the key activities within the International Civil Aviation Organisation (ICAO). As from 9/11, ICAO has become extremely active in security awareness and support, facilitation, training and oversight. Provisions for international aviation security were first disseminated as Annex 17 to the Chicago Convention in 1974 and since then have been improved and updated 11 times. A 12th amendment to the Annex has been approved by the ICAO Council and is applicable since 1 July 2011. For the first time, this amendment will incorporate provisions for ATM security and cyber security. An improved Aviation Security Manual (Eighth Edition – 2011) has also been published to support States to implement Annex 17 SARPs.

Current activities relevant to ATM security are:

- Development of an ATM Security manual covering both the self-protection and the collaborative support ATM security areas;
- Security threat and risk assessments, in order to carry out a gap analysis of Annex 17, to include the full spectrum of threats to aviation security.

A fundamental element within the ICAO Aviation Security Programme is the ICAO Universal Security Audit Programme (USAP). It represents an important initiative in ICAO's strategy for strengthening aviation security worldwide and for attaining commitment from States in a collaborative effort to establish a global aviation security system.

The programme, part of ICAO's Aviation Security Plan of Action, provides for mandatory and regular audits of all ICAO Contracting States. The ICAO audit assesses the State's capability for providing security oversight by determining whether the critical elements of a security oversight system have been implemented effectively. Thus, the USAP serves to promote global aviation security by identifying weaknesses in each State's oversight of its aviation security activities and, if required, providing suitable recommendations for mitigating or resolving such shortcomings.

Implementation of the programme began with the first security audit in November 2000. The second cycle of security audits commenced in January 2008 and is expected to conclude in 2013. In addition to security audits, the programme entails audit follow-up visits that focus on the implementation of corrective action plans.

To promote transparency and mutual confidence between States, information on the level of implementation of the critical elements of an audited State's aviation security oversight system is available to all ICAO Member States on a restricted web site.

It could be expected that ATM Security and Cyber Security (included in amendment 12 of Annex 17) would be incorporated in the USAP in a near future. This would have an impact on the national ATM Security Oversight Programme.

## 5.2 The European Regulatory Framework (SES I/SES II and AVSEC)

The initial SES package came into force in 2004. In the light of the SES, a specific regulatory framework for Air Navigation Service (ANS) Security has been developing in the European Union since 2004 (e.g. Regulation (EC) N° 550/2004, 552/2004 and Regulation (EC) N° 1035/2011).

The Service Provision Regulation (EC) N° 550/2004 establishes common requirements for the safe and efficient provision of ANS in the Community where security is one of requirements. The regulation includes a common system for the certification and designation of air navigation service providers. This enables the definition of their governing rules and obligations.

The objective of Regulation (EC) N° 552/2004 on the interoperability of the European Air Traffic Management network is to achieve interoperability between the different systems, constituents and associated procedures of the EATMN, taking due account of the relevant international rules. This regulation also aims at ensuring the coordinated and rapid introduction of new agreed and validated concepts of operations or technology in air traffic management. One of the essential requirements laid down in the regulation is civil-military coordination. In this regard, the regulation states that *'account should be taken of national security requirements'*.

Civil and military system interoperability is not only a security requirement but an enabler. The ATM security collaborative support function (see chapter 3.3, Understanding ATM Security) requires information exchange between civil ATM and national authorities responsible for ATM and airspace security.

System, constituent and procedure interoperability is also an essential requirement in a net-centric environment where real-time information exchange of information will enable the expected SES performance.

Therefore, the interoperability regulation could be considered as an enabler for security.

The SES regulatory framework is distinct from the regulatory framework for aviation security (i.e. former Regulation (EC) N° 2320/2002 and new Regulation (EC) N° 300/2008).

The Regulation (EC) N° 550/2004, on the provision of air navigation services in the single European sky, lists security as one of the common requirements for the provision of air navigation services. The Regulation (EC) N° 1070/2009, also known as the SES II package, amended the Framework Regulation (EC) No 549/2004, laying down the framework for the creation of the single European sky, and became a fundamental enabler for the realisation of the SES. Currently the SES II package is in the process to be amended. A proposal has been developed by the European Commission and will be submitted to the European Parliament for approval. Still, it is not known what impact the proposed regulation will have on security issues.

Regulation (EC) N° 1108/2009 amending Regulation (EC) N° 216/2008 in the field of aerodromes, air traffic management and air navigation services extends the competencies of EASA to aerodromes and ATM/ANS (see chapter 6.2.2.1). New proposed amendments to Regulation (EC) N° 216/2008 foresee a new article relating to the safety rules on the protection of classified and sensitive non-classified information.

### **5.2.1 Security Aspects of Regulation (EC) N° 1035/2011**

Air Navigation Service Security is regulated by the Commission Implementing Regulation (EU) N° 1035/2011 (repealing 2096/2005), 'laying down common requirements for the provision of air navigation services'. As stated in paragraph above, the National Supervisory Authorities (NSA) have the obligation to organise inspections and surveys to verify compliance with those requirements (Service Provision Regulation (EC) N° 550/2004).

#### **5.2.1.1 Security Management Systems**

Annex I, General requirements for the provision of air navigation services, establishes a security requirement, namely:

*An air navigation service provider shall establish a security management system to ensure:*

*(a) the security of its facilities and personnel so as to prevent unlawful interference with the provision of services;*

*(b) the security of operational data it receives or produces or otherwise employs, so that access to it is restricted only to those authorised.*

*The security management system shall define:*

*(a) the procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;*

*(b) the means designed to detect security breaches and to alert personnel with appropriate security warnings;*

*(c) the means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.*

*An air navigation service provider shall ensure the security clearance of its personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data.*

*The safety, quality and security management systems may be designed and operated as an integrated management system.*

It must be noted that regarding the protection of data the requirement that access to it is restricted only to those authorised refers to the Confidentiality of information. The basic three information security requirements are: Confidentiality, Availability and Integrity (CIA).

#### **5.2.1.2 Contingency Plans**

Air navigation service providers shall have in place contingency plans for all air navigation services they provide in the case of events which result in significant degradation or interruption of their operations.

#### **5.2.1.3 Other Security Aspects**

The regulation, in its Annex I, lists General Requirements (Security being one of them) and in its Annex II Specific Requirements for the provision of air navigation services. Among the specific ones, it mentions requirements for the provision of Meteorological Services, Aeronautical Information Service and Communication, Navigation and Surveillance Services.

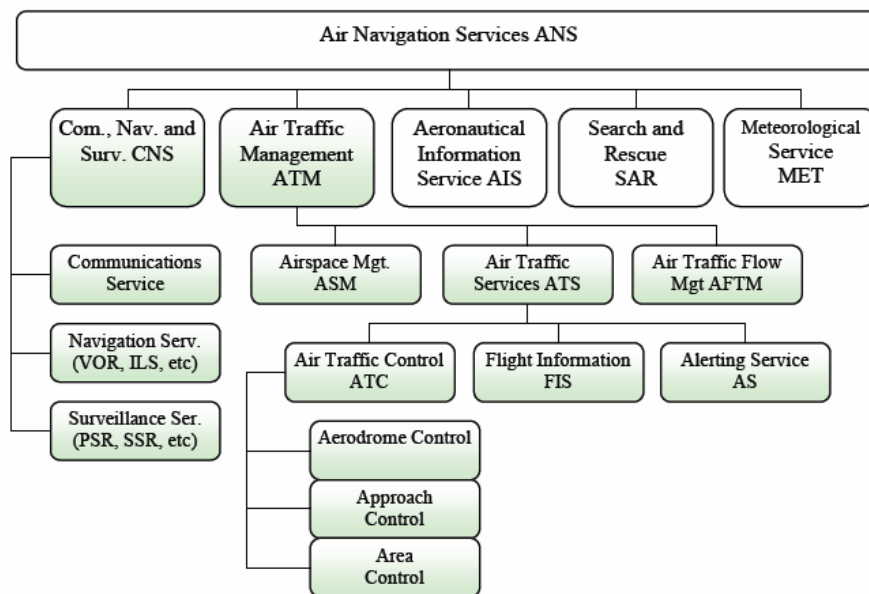


Regarding the provision of Aeronautical Information Service, the regulation states that: ‘A provider of aeronautical information services shall ensure the **integrity of data** and confirm the level of accuracy of the information distributed for operations, including the source of such information, before such information is distributed’.

Regarding the provision of Communication, Navigation and Surveillance Services the regulation states that: ‘A provider of communication, navigation or surveillance services shall ensure the **availability**, continuity, accuracy and **integrity** of its services’.

As mentioned before availability and integrity are, together with confidentiality, the three basic information security (INFOSEC) requirements (**CIA**). Nevertheless, the text does not mention if these CIA requirements are against security (intentional threats). This is important since the **safety/security interface** in ATM security and mainly in cyber security is an area that needs to be addressed.

These dispersed elements **do not provide a consistent INFOSEC requirement** per se. However, considering all together in the framework of air navigation services, it can not be neglected that INFOSEC aspects are partially addressed. The ICAO breakdown of air navigation services is included below as reference. The security oversight responsibilities **extend to all** these aspects of ANS.



**Figure 8: Air Navigation Services**

### 5.2.2 Security Aspects of Regulation (EC) N° 73/2010

Regulation (EC) N° 73/2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky, lays down the requirements on the quality of aeronautical data and aeronautical information in terms of accuracy, resolution and integrity. As already said, **integrity** is one of the CIA requirements. Furthermore, Annex VII, Part C to the regulation, list Security management objectives:

- Ensure the security of aeronautical data and aeronautical information received, produced or otherwise employed so that it is protected from interference and access to it is restricted only to those authorised;
- Ensure that the security management measures of an organisation meet appropriate national or international requirements for critical infrastructure and business continuity, and international standards for security management, including the ISO standards referred to hereafter.

Regarding the ISO standards, the relevant certificate issued by an appropriately accredited organisation, shall be considered as a sufficient means of compliance.

ISO referred to:

- International Organisation for Standardisation, ISO/IEC 17799:2005<sup>7</sup> — Information technology — Security techniques — Code of practice for information security management (Edition 2 — 10.6.2005)
- International Organisation for Standardisation, ISO 28000:2007: — Specification for security management systems for the supply chain (Edition 1 — 21.9.2007 under revision, to be replaced by Edition 2 target date 31.1.2008 [At enquiry stage])
- Other initiatives in Europe, like the 'Information Security Standards for Aviation Organisations', point at the same direction; promoting the use of ISO for ICT security. It should be welcomed since it could provide the general baseline and grounds for harmonised INFOSEC in aviation. However, caution should be raised before considering ISOs as the complete or definite solution for cyber defence in the SES.

### **5.2.3 Security Aspects of Regulation (EC) N° 300/2008 (not SES related)**

Regulation (EC) N° 300/2008 on common rules in the field of civil aviation security applies to airports and aircraft operators. This regulation establishes, inter alia, the following security requirements:

- Member States shall designate a single civil aviation authority, even if two or more bodies are involved in civil aviation security;
- Every Member State shall draw up, apply and maintain a national civil aviation security programme;
- Every Member State shall draw up, apply and maintain a national quality control programme;
- Every airport operator shall draw up, apply and maintain an airport security programme;
- Every air carrier shall draw up, apply and maintain an air carrier security programme;
- Every entity required under the national civil aviation security programme to apply aviation security standards shall draw up, apply and maintain a security programme;
- The Commission, acting in cooperation with the appropriate authority of the Member State concerned, shall conduct inspections, including inspections of airports, operators and entities applying aviation security standards, in order to monitor the application by

---

<sup>7</sup> The current name of the standard is ISO 27002

Member States of this Regulation and, as appropriate, to make recommendations to improve aviation security;

- Common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation. Most of these common standards refer to security on the ground. However, there are also 'IN-FLIGHT SECURITY MEASURES', namely:

1. Without prejudice to the applicable aviation safety rules:

- (a) unauthorised persons shall be prevented from entering the flight crew compartment during a flight;
- (b) potentially disruptive passengers shall be subjected to appropriate security measures during a flight.

2. Appropriate security measures such as training of flight crew and cabin staff shall be taken to prevent acts of unlawful interference during a flight.

3. Weapons, with the exception of those carried in the hold, shall not be carried on board an aircraft, unless the required security conditions in accordance with national laws have been fulfilled and authorisation has been given by the States involved.

4. Paragraph 3 shall also apply to in-flight security officers if they carry weapons.

These in-flight security measures should be considered as part of the ATM Security/Self-Protection area. But still they keep an indirect link with ATM security/Collaborative Support and Airspace Security since they can prevent a hijack or RENEGADE situation.

Regulation (EC) N° 300/2008 provides elements for a security framework; authority, organisation, structure, roles and responsibilities, security programmes, oversight mechanisms, etc. Considering that Aviation Security is the placeholder for all security components related to civil aviation, this regulation could well accommodate ATM security requirements as well. Furthermore, many ATM facilities reside within the remits of airports. The misunderstanding that aviation security refers exclusively to airport security should be avoided.

### **5.3 The National Regulatory Framework**

National regulations complementing or extending global and regional regulations and standards are extremely important in order to adapt the regulatory framework to local circumstances. Each State should tailor or customise the international security framework to its specific needs and constraints. National security regulations are especially relevant in the case of the ATM Security/Collaborative Support area. This is because the link with national security and defence precludes any regulatory activity other than national. Nevertheless, the international dimension of ATM security imposes the adoption of a harmonised global approach and the uniform and effective application of suitable measures. Organisations like EUROCONTROL, NATO and ICAO (now addressing civil military cooperation in ATM) play a role in this regard.

The most critical aspect of the ATM collaborative support is the provision of information to the national civil and military authorities (e.g. Air Defence) and the support in case of security incidents (collaborative ATM security incident management). Following the 9/11 attacks, many States nominated a National Governmental Authority (NGA) (see Annex C)

responsible for the decision-making and resolution of air space security incidents, like RENEGADE<sup>8</sup>. Accordingly, many States have reviewed or issued new legislation to cope with the new threat.

The implementation of this legislation must also be part of the national ATM security oversight programme (see Annex D, security questionnaires).

## 6. GOVERNANCE AND ORGANISATION

Governance is the **enabler for trust** and trust is the enabler for security. To build up a robust trust model, **governance** aspects are key. Security encompasses very complex multidisciplinary elements; physical, organisational, personnel and technical security aspects across a large variety of stakeholders; airspace users, air navigation service providers, authorities, supervisors, etc.

**Security governance** must be based on:

- Agreed security framework;
- Agreed legal framework;
- Security policy definition, enforcement and maintenance;
- Security system definition and implementation;
- Clear roles and responsibilities at national and user/entity level;
- Certification, accreditation and authorisation mechanisms (for people and systems);
- Global security management under a single security authority;
- Crisis/incident management procedures;
- Assurance framework: arrangements, monitoring, inspections and audits;
- Validation and implementation of corrective security measures;
- Change management for improved security;
- Liability issues, infringements, investigations and penalties;
- Education, awareness and training arrangements.

### 6.1 Governance

Aviation security is a **national responsibility** and therefore, a number of authorities and departments are involved in different ways. Nevertheless, the **international dimension** of aviation and ATM security also imposes the adoption of a harmonised global approach and the uniform and effective application of suitable measures.

---

<sup>8</sup> A situation where a civil aircraft is used as weapon to perpetrate a terrorist attack is usually referred to as a RENEGADE

## 6.1.1 Roles and Responsibilities in Aviation Security

### 6.1.1.1 Global Level

ICAO (International Civil Aviation Organisation). As already mentioned in paragraph 5.1, Aviation Security is one of the **key activities** within ICAO. In 2001, both the Annex 17 and its Aviation Security Manual have been updated. The most relevant change relates to cyber security (new SARPs in Annex 17 and Chapter with guidance in the AVSEC Manual, Doc 8973–Restricted). At the end of 2012, the ICAO ATM Security Manual, Doc 9985-AN/492 – Restricted was published. It complements the AVSEC Manual and provides guidance on security issues specific to ATM in order to assist States and ANSPs in implementing appropriate security provisions to meet the published requirements of the NCASP. In addition, the manual provides guidance to the ANSPs on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities.

### 6.1.1.2 European Level

The European Commission (EC). The European Commission (EC) is the **single European regulator** for aviation, thus for aviation and ATM security. Aviation security issues are dealt within DG/MOV Unit E5 (Aviation Security). Aviation security is the overall framework where ATM security is a fundamental part. The Unit responsible for ATM security is DG/MOVE2, Single European Sky. The possible misunderstanding that aviation security refers exclusively to airport security should be avoided. All the AVSEC components relate to each other and should be considered in a holistic way.

The reference legislation is Regulation EC N° 300/2008 on common rules in the field of civil aviation security. According to it the Commission, acting in cooperation with the appropriate authority of the Member State concerned, shall conduct inspections, including inspections of airports, operators and entities applying aviation security standards, in order to monitor the application by Member States of this Regulation.

An important aspect of the Regulation is the possibility to reach agreements recognising that the security standards applied in a third country are equivalent to Community standards, in order to advance the goal of ‘one-stop security’ for all flights between the European Union and third countries. This is also very relevant in regard to the air cargo security issues.

The European Aviation Safety Agency (EASA). EASA was created by Regulation (EC) N° 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency (Basic Regulation).

EASA is responsible for ensuring that the EU aviation safety legislation is properly, uniformly and consistently implemented. This role covers inspections for standardisation of the National Civil Aviation Authorities (CAAs). In addition, inspections to CAAs are also performed by the Agency in the context of the accreditation process for allocation of certification tasks. The Agency also focuses on the approval and oversight of organisations, specifically the Design, Production, and Continued Airworthiness Organisations, within the scope of Article 20 of the EASA Basic Regulation. The Agency carries out Standardisation Inspections in EASA Member States in accordance with Commission Regulation (EC) N° 736/2006 on working methods of the European Aviation Safety Agency for conducting standardisation inspections (see Appendix 4, paragraph 4).

Regulation (EC) N° 1108/2009 amending Regulation (EC) N° 216/2008 in the field of aerodromes, air traffic management and air navigation services extends the competencies of EASA to aerodromes and ATM/ANS. In the last case, the regulation is applicable to:

1. The design, production and maintenance of systems and constituents for air traffic management and air navigation services (ATM/ANS) as well as personnel and organisations involved therein;
2. ATM/ANS as well as personnel and organisations involved therein.

It means that EASA standardisation inspections will cover the requirements laid down in Commission Implementing Regulation (EU) N° 1035/2011; this includes security and contingency requirements.

New proposed amendments to Regulation (EU) N° 216/2008 foresee a change of the Agency name into 'European Union Agency for Aviation', with new responsibilities which might have an impact on security.

The European Civil Aviation Conference (ECAC). Security is one of the three strategic priorities of ECAC and represents a key activity area of the organisation. Maintaining high security standards, while at the same time anticipating new and emerging threats, are serious challenges facing all Member States and the industry. In this context, ECAC's security activities are multi-faceted: they include the development of recommendations and good practices by several groups, and the management and implementation of four operational programmes.

ECAC has been very active in security since 9/11. Its famous Doc. 30 (AVSEC Standards) was issued early 2002. Recently, the document has been updated (13<sup>th</sup> Edition, May 2010) to include ATM security provisions, provided by EUROCONTROL, for both self-protection and collaborative support ATM security areas. Doc. 30 also includes a chapter on cyber security.

ECAC is also very active in promoting cooperation with other regions and non-ECAC Member States, fostering mutual understanding on their respective security organisation and measures, by supporting regional initiatives and organising joint activities.

### **6.1.1.3 National Level**

National level committees, authorities and related organisations are described in Annex C.

### **6.1.2 Specific Roles and Responsibilities in ATM Security at National Level**

The table below provides a summary template of the different main roles and responsibilities in ATM security at national level. It includes both aspects: self-protection and collaborative support (see paragraph 3.3) of ATM security. A more exhaustive description of roles and responsibilities at national level is included in Annex 1.

Scenario	EC	CAA/NSA	ANSP/Network Manager (NM)	National Authorities	Aircraft Operators (AO)
<b>Self-protection</b> (Physical security, personnel security, cyber security)	<ul style="list-style-type: none"> <li>• Legislation</li> <li>• External agreements (ICAO, 3<sup>rd</sup> countries)</li> <li>• Oversight (EASA?)</li> </ul>	<ul style="list-style-type: none"> <li>• Regulations</li> <li>• Accreditation, designation</li> <li>• Issue/control of licenses and certificates for ATM (pilots, controllers)</li> <li>• Contingency planning for civil aviation</li> <li>• Security oversight</li> </ul>	<ul style="list-style-type: none"> <li>• Implementation of SeMS</li> <li>• Security procedures</li> <li>• Crisis management/contingency plans</li> <li>• Coordination with national civil and military authorities</li> </ul>	<ul style="list-style-type: none"> <li>• Intelligence (threat assessment and warning)</li> <li>• Security control of small airfields</li> <li>• Protection and Intervention (at airport)</li> <li>• Air marshals</li> </ul>	<ul style="list-style-type: none"> <li>• In-flight security measures</li> <li>• Airport security measures (air side)</li> </ul>
Scenario	EC Role	CAA/NSA	ATM Role (ANSP/NM and AO)	Police/Security Forces Role	NGA <sup>9</sup> /Military
<b>Collaborative support</b> (e.g. RENEGADE)	<ul style="list-style-type: none"> <li>• Legislation</li> <li>• External agreements (ICAO, 3<sup>rd</sup> countries)</li> </ul>	<ul style="list-style-type: none"> <li>• Regulations</li> <li>• Airspace design</li> <li>• Control of licenses and certificates for ATM</li> <li>• Contingency planning for civil aviation</li> </ul>	<ul style="list-style-type: none"> <li>• Security of Flight Plan process</li> <li>• Positive identification of flights</li> <li>• Crew/cargo/passenger information</li> <li>• Triggering and information on incidents e.g. situation on board</li> <li>• Security</li> </ul>	<ul style="list-style-type: none"> <li>• Intelligence (threat assessment and warning)</li> <li>• Security control of small airfields</li> <li>• Intervention (at airport)</li> <li>• Air marshals</li> </ul>	<ul style="list-style-type: none"> <li>• Legislation</li> <li>• Decision-making e.g. closing of airspace, aircraft intervention</li> <li>• Crisis management</li> <li>• Cross-border cooperation</li> <li>• Air Surveillance (detection and identification)</li> <li>• Intelligence and threat</li> </ul>

<sup>9</sup> NGA: National Governmental Authority

			<p>procedures</p> <ul style="list-style-type: none"> <li>• Crisis management e.g. airspace and flow management measures</li> </ul>		<p>assessment</p> <ul style="list-style-type: none"> <li>• Temporary Flight Restrictions</li> <li>• Civil-military coordination</li> <li>• Cross-border coordination</li> <li>• NGA structure</li> <li>• Air Defence: Intervention/engagement (national responsibility)</li> </ul>
--	--	--	--	--	--

**Table 1: Roles and Responsibilities in ATM Security**

**6.1.3 Consultation**

One very important element of ATM security is the international consultation process. Expert bodies contributing to ATM security developments are:

- The NATO EUROCONTROL ATM Security Coordinating Group (NEASCOG)
- The EUROCONTROL ATM Security Team (SET)

Other consultation bodies in aviation security are:

- ICAO Aviation Security Panel;
- ECAC Security Forum and its Guidance Material Task Force and Study Group on cyber threats to civil aviation;
- EC Aviation Security Regulatory Committee;
- SAGAS (Stakeholders Advisory Group on Aviation Security), as per Regulation (EC) N° 300/2008.

The ATM security authorities must be aware of who are the national representatives in all the above security fora. Furthermore, it is required that all national representatives speak with a single voice and pass the same message in line with national security policy. This policy and subsequent **coordinated** security positions must be established at the level of the National Civil Aviation Security Committee, NCASC (see Annex C).

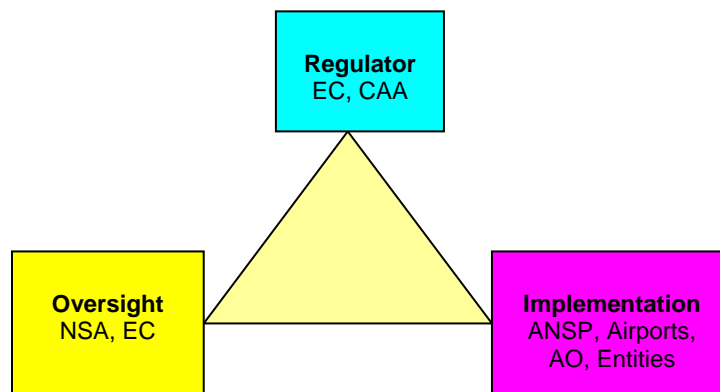


## 7. OVERSIGHT PROGRAMME

Security oversight is a key element in the overall security process. It is the responsibility of the State security authorities. Security oversight guarantees security compliance, and therefore contributes to improve the trust framework.

It also facilitates the security assurance and validation process on the part of the organisations implementing the security requirements and helps improve the security loop Plan-Do-Check-Act, thus enhancing the quality of the security management systems.

Security oversight is one of the three main aspects of a system approach to security, the other two being the regulatory and the provision (or implementation) functions, as depicted in the triangle in the figure below.



**Figure 9: Separation of Regulatory, Oversight and Implementation Functions**

When developing an ATM Security Oversight Programme, the following elements should be considered:

- **Scope:** The ATM Security Oversight Programme must be an integral part of the overall National AVSEC Programme (through the National Quality Control Programme), as ATM security is a component of the overall Aviation Security concept;
- **Authority:** a single authority must be responsible for the National ATM Security Oversight Programme; NSA (National Supervisory Authority). Role or links with other authorities responsible for security must be clarified i.e. CAA, AA, NGA;
- **Organisation:** list of entities in the provision/implementation side of the triangle, which are subject of security oversight by the NSA. Agreed generic process:
  - Threat and Risk Assessment; what are the threats to the ATM system?
  - Audit/inspection programme; annual plan, coordination, preparations
  - Verification of compliance/desktop; pre-visit activities
  - Oversight of compliance on-site; on-site inspection

- Resulting actions; audit reports, oversight record archive, resolution of non-conformities, follow-up and conclusion of oversight, conclusions of conformities and non-conformities, monitoring ongoing compliance/improve.
- **Audit/Inspections Plan:** it must be developed on an annual basis, in coordination with the organisations to be audited. It should include:
  - Schedules;
  - Pre-visit questionnaires;
  - Pending actions resulting from last inspections;
  - On-site audit check lists and;
  - Coordination details.

Generic guidance for oversight of Security Management Systems is provided in Annex D.

- **Current Status:** before initiating a security oversight process it is recommendable to have an overview on the current status of ATM security within the country, including possible regulatory gaps. NSA Self Assessment Questionnaires are provided in Annex D in support of this assessment.
- **Process**

A generic ATM security oversight process is provided in Appendix 4 to Annex D, security oversight programme.

## ANNEX A – Acronyms

AA	Appropriate Authority
ACA	Airspace Control Authority
ACC	Area Control Centre
ADS-B	Automatic Dependent Surveillance Broadcast
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
AO	Aircraft Operator
ASA	Air Service Agreement
ASSIM	Airspace Security Incident Management
ATM	Air Traffic Management
ATS	Air Traffic Services
AVSEC	Aviation Security
FAB	Functional Airspace Block
CAA	Civil Aviation Authority
CIA	Confidentiality, Integrity and Availability
CIP	Critical Infrastructure protection
CNS	Communications, Navigation, Surveillance
CIIP	Critical Information Infrastructure Protection
CAOC	Combined Air Operations Centre
COMLOSS	Communication Loss
COMSEC	Communication Security
COTS	Commercial Off-The-Shelf
DoD	Department of Defence
EASA	European Aviation Safety Agency
EACCC	European Aviation Crisis Coordination Cell
EC	European Commission
ECAA	European Common Aviation Area
ECAC	European Civil Aviation Conference
FAA	Federal Aviation Administration
FAB	Functional Airspace Block
GNSS	Global Satellite Navigation System
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technologies
INFOSEC	Information Security

MAA	Military Aviation Authority
MANPADS	Man Portable Air Defence System
NAA	National Aviation Authority
NATO	North Atlantic Treaty Organisation
NCASC	National Civil Aviation Security Committee
NCASP	National Civil Aviation Security Programme
NCASQCP (or NQCP)	National Civil Aviation Security Quality Control Programme
NCASTP	National Civil Aviation Security Training Programme
NEASCOG	NATO-EUROCONTROL ATM Security Coordinating Group
NGA	National Governmental Authority
NM	Network Manager
NSA	National Supervisory Authority
NSecA	National Security Authority
PoC	Person of Contact
PPP	Public Private Partnership
R&D	Research and Development
SARPs	Standards and Recommended Practices (ICAO)
SeMS	Security Management System
SES	Single European Sky
SESAR	Single European Sky Air Traffic Management Research
SET	ATM Security Team
SJU	SESAR Joint Undertaken
SWIM	System Wide Information Management
SQL	Structure Query Language
UAS	Unmanned Aerial System
USAP	Universal Security Audit Programme

## ANNEX B – Definitions

**Acts of Unlawful Interference** - Acts or attempted acts such as to jeopardise the safety of civil aviation, including but not limited to:

- Unlawful seizure of aircraft;
- Destruction of an aircraft in service;
- Hostage-taking on board aircraft or on aerodromes;
- Forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- Introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes;
- Use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment; and
- Communication of false information such as to jeopardise the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

**Air Navigation Service Provider (ANSP)** - The organisation that provides air traffic management (used interchangeably with the term “air traffic service provider (ATSP)” in ICAO context).

**Airspace Security** - The safeguarding of the airspace of responsibility from unauthorised use, intrusion, illegal activities or any other violation. This involves managing the airspace to prevent, detect and resolve where possible airborne threats.

**Airspace Management for ATM Security** - Management of the airspace to: 1) deter, prevent, detect and resolve where possible airborne threats; 2) provide for emergency security control of air traffic; and 3) initiate and monitor temporary flight restrictions in support of national security and law enforcement activities.

**Air Traffic Management (ATM)** - The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management - safely, economically and efficiently - through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground based functions.

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

**ATM Security System** - A combination of organisation, means and doctrine (regulations and procedures) established to protect the ATM system.

**ATM System** - A system that provides ATM through the collaborative integration of humans, information, technology, facilities, and services, supported by air and ground and/or space based communications, navigation and surveillance<sup>10</sup>.

**Airspace Security Incident** - A situation where the behaviour of a flight matches the agreed security criteria needed to initiate security coordination and actions.

**ATM System Infrastructure** - ATM System infrastructure includes people, procedures, information, resources, facilities, including control centres, and airports, and equipment, including CNS and information systems.

**ATM System Infrastructure Protection** - The protection of the ATM system infrastructure through communication security, information security, physical security and personnel security measures.

- **Information Security (INFOSEC)**

The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security. Such measures also include detection, documentation and countering of threats to information and to systems.

(1) Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) Confidentiality means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability means ensuring timely and reliable access to and use of information.

- **Communications Security (COMSEC)**

The application of security measures to telecommunications in order to deny unauthorised persons information of value which might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

*Note:* Such measures include crypto, transmission and emission security, and also include procedural, physical, personnel, document and computer security.

- **Physical Security**

That part of security concerned with physical measures designed to safeguard people; to prevent unauthorised access to equipment, facilities, material, and documents; and to safeguard them against a security incident.

---

<sup>10</sup> It is important to note that a system does not necessarily stand for a sophisticated tool or state of the art hardware and software. On the contrary, often it just encompasses elements, activities, people or ideas.

- **Personnel Security**

That part of security concerned with procedures designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorised to have initial and continued access to classified information without constituting an unacceptable risk to security.

**Aviation Security** - Safeguarding of civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human resources.

**Aviation Security Oversight** - Function as means of which States **ensure** the effective implementation of security-related SARPs and associated procedures contained in the Annexes to the Chicago Convention.

**Contingency Plan** - A proactive plan to include measures and procedures addressing various threat levels, risk assessments and the associated measures to be implemented, designed to anticipate and mitigate events as well as prepare all concerned parties having roles and responsibilities in the event of an actual act of unlawful interference. A contingency plan sets forth incremental security measures that may be elevated as the threat increases. It may be a stand alone plan or included as part of a Crisis Management Plan.

**Crisis Management** – Contingency measures implemented in response to increased threat levels as well as implementation of measures and procedures in response to the emergencies to include acts of unlawful interference.

**Cyber Security** - It is the ability of the organisation to through the application of safeguard measures and actions secure its people, information, systems and reputation in cyberspace in civil and military fields. Cyber-security strives to preserve the availability and integrity of networks and infrastructure, and the confidentiality of the information contained therein.

**RENEGADE** - A situation where a civil aircraft is used as weapon to perpetrate a terrorist attack is usually referred to as a RENEGADE.

**Risk** - Potential for an unwanted outcome resulting from an incident, event, or occurrence. Risk can be estimated by considering the likelihood of threats, vulnerabilities and consequences or impact.

**Risk Assessment** - Continual, ongoing exercise to update the complete range, magnitude and type of credible threats and their likelihood, based on reliable information from the intelligence services, the vulnerabilities to them, and the possible consequences or impact of loss or degradation from successful attacks.

**Security** - The condition achieved when designated information, material, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorised disclosure.

**Security audit** - An in-depth compliance examination of all aspects of the implementation of the national civil aviation security programme.

**Security control** - A means by which the introduction of weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference can be prevented.

**Security inspection** - An examination of the implementation of relevant national civil aviation security programme requirements by an airline, ANSP, airport or other entity involved in security.

**Security investigation** - An inquiry into any act or attempted act of unlawful interference against civil aviation and/or any alleged or suspected instance of non-compliance with the State's National Civil Aviation Security Programme or other legal and/or regulatory requirements pertaining to civil aviation security.

**Security Monitoring**

- Supervising security activities in progress to ensure they are compliant with the security requirements and on-course and on-schedule in meeting the security objectives and performance targets.
- Network Security Monitoring is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions.

**Security Programme** - Written measures adopted to safeguard international civil aviation against acts of unlawful interference.

**Security Supervision** - Observation, direction and inspection of the execution of (a security task or activity) or the security work of (a person) normally by a superior.

**Security Survey** - An evaluation of security needs including identification of vulnerabilities which could be exploited to carry out an act of unlawful interference, and the recommendation of corrective actions.

**Security Test** - A covert or overt trial of an aviation security measure which simulates an attempt to commit an unlawful act.

**Terrorism** - The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.

**Threat** - Measure of the likelihood or probability of an attack being attempted against a particular target within a specified time frame. Threats are deliberate, intentional acts carried out by individuals or organisations, generally with a hostile purpose. The likelihood is a function of the terrorist's means or capability to act, their motivation to do so and their intention to do so.

**Vulnerability** - Those characteristics of a target which could be exploited in an attack. Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or attack or susceptible to a given hazard.



## ANNEX C – Roles and Responsibilities in ATM Security

### Appropriate Authority (AA)

At national level, the focal point in aviation security is the National Civil Aviation Security Authority, referred to as the Appropriate Authority (AA). ICAO Annex 17 establishes that Each Contracting State shall designate and specify to ICAO an appropriate authority within its administration to be responsible for the development, implementation and maintenance of the national civil aviation security programme (NCASP).

This programme aims at safeguarding civil aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights.

The appropriate authority is responsible:

- to define and allocate tasks and coordinate activities between the departments, agencies and other organisations of the State, airport and aircraft operators, air traffic service providers and other entities concerned with or responsible for the implementation of various aspects of the national civil aviation security programme;
- Establish a national aviation security committee or similar arrangements for the purpose of coordinating security activities between the departments, agencies and other organisations of the State, airport and aircraft operators, air traffic service providers and other entities concerned with or responsible for the implementation of various aspects of the national civil aviation security programme;
- To ensure the development and implementation of a national training programme for personnel of all entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme. This training programme shall be designed to ensure the effectiveness of the national civil aviation security programme;
- To develop, implement and maintain a national civil aviation security quality control programme to determine compliance with and validate the effectiveness of its national civil aviation security programme. The Appropriate Authority shall arrange for security audits, tests, surveys and inspections to be conducted on a regular basis, to verify compliance with the national civil aviation security programme and to provide for the rapid and effective rectification of any deficiencies;
- Regulation (EC) N° 300/2008 also refers to the Appropriate Authority: 'where, within a single Member State, two or more bodies are involved in civil aviation security, that Member State shall designate a single authority (referred to as the appropriate authority) to be responsible for the coordination and monitoring of the implementation of the common basic standards for aviation security'.

National Appropriate Authority				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**The National Civil Aviation Security Committee (NCASC)**

The NCASC plays a fundamental role given the large number of government departments and agencies likely to be involved in aviation security activities within a State (e.g. Transport, Defence, Interior, Foreign Affairs, Intelligence, Customs, etc). It is imperative to facilitate ongoing coordination among these key players. This is achieved by means of the NCASC or similar arrangements. The NCASC should be a standing committee that meets regularly, acting under the authority of the government. In order to ensure decisive action, the NCASC should consist of senior government officials and senior representatives of the aviation industry, the latter acting as consultants to the government. Ideally, NCASC meetings should take place at least twice per calendar year. The following recommendations concern the NCASC composition:

- a) When the NCASC is to discuss matters related to preventive measures and procedures and other associated actions, it would be appropriate for the chair to be a senior official of the State’s department or agency responsible for civil aviation. On those occasions when contingency plans and associated actions in response to an occurrence are to be discussed, it would be appropriate for the chair to be a senior official of the State’s department or agency responsible for such planning and actions. Ministries or agencies to be represented on the committee should include, but are not necessarily limited to, the CAA, the MAA (Military Aviation Authority), security forces and services, the authority responsible for police functions, immigration, customs, other border control agencies, postal services and external relations.
- b) As a minimum, the chair of the national facilitation committee should be a member of the NCASC to ensure consistency in programme implementation and to consider possible effects of security measures on day-to-day aviation operations.
- c) The committee should also invite additional members, on an ad hoc basis and as considered necessary, from airport administrations, aircraft operators, ANSP and employee organisations, particularly those representing crew members and personnel responsible for air traffic services and for communications, so as to ensure that adequate operating technical expertise and experience are available during its deliberations.

Depending on how services are structured in a particular State, this may include (in addition to the appropriate authority for civil aviation security) members from the following organisations (list not exhaustive):

- ANSPs
- Aircraft operators
- Airport operators
- General aviation

- Transport authorities
- Customs authorities
- Immigration authorities
- Law Enforcement authorities
- Security authorities e.g. National Security Authorities and cyber security
- Military
- Intelligence organisations
- Critical infrastructure protection
- Providers of contracted security services

In addition to the NCASC, ICAO Annex 17 (Security) requires the establishment of an airport security committee for each civil airport.

This collaborative, cooperative approach is necessary to ensure that security policies and provisions will be able to successfully counter the whole range of threats to aviation.

National Civil Aviation Security Committee members				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**National Governmental Authority (NGA)**

In every State within NATO context, there is an authority nominated who is responsible for the decision-making in case of serious airborne threat to national interests (e.g. 9/11 type, RENEGADE aircraft). The NGA is at very high level (e.g. Prime Minister or Minister) and is in permanent contact with the Air Defence Chain of Command (National Air Defence Commander), who is responsible for airspace security actions and air contingency planning. The air defence system establishes coordination links with other departments (e.g. Interior) and ATM players; ANSP, Aircraft Operators and Airport Operators, who provides support to the national civil and military authorities in all phases of a security event.

National Governmental Authority				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**National Security Authority (NSecA)**

The National Security Authority (also known as NSA in the security world) is another high level governmental authority among others responsible for:

- granting security clearances to all national personnel requesting so. It includes security clearances in the framework of international treaties and agreements e.g. NATO. He/she is also responsible for vetting procedures and security investigations according to national legislation and procedures;
- accreditation and audit of national security systems for the protection of classified information;
- accreditation and audit of national information security (INFOSEC) systems and networks for the transmission of sensitive and classified information. It includes crypto systems and keys management.

The functions of the NSecA are relevant to ATM in the light of:

- Regulation EC N° 1035/2011 requirement for ANSP to *ensure the security clearance of its personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data;*
- The future SWIM security environment, where robust security policies e.g. for personnel security will have to be implemented.

National Security Authority				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**The Civil Aviation Authority (CAA)**

The CAA is the aviation regulator in every State, and is therefore responsible for developing security regulations for civil aviation. It includes regulations and policies for Airports, ANSP, Aircraft Operators, General Aviation, Manufacturers, etc.

National Civil Aviation Authority				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**The National Supervisory Authority (NSA)**

The NSA is established by the SES Framework Regulation and is responsible for the oversight of the national air navigation system. The NSA is also responsible for issuing certificates to air navigation service providers where they comply with the common requirements referred to in Commission Implementing Regulation (EU) N° 1035/2011.

The CAA, NSA and Appropriate Authority are nominated by the State. They should normally belong to the Ministry of Transport. Nevertheless, States might decide otherwise, for instance the oversight function can be assigned to a higher level when it includes national police or military involved in the protection of critical infrastructure e.g. hubs, radar and communications sites.

It is normal practice that the CAA will also perform as the NSA. Normally, the Appropriate Authority is at present only involved in airport security issues. Nevertheless, the new amendment of ICAO Annex 17 requires including ANS (ATS in ICAO terminology) within the National Civil Aviation Security Programme (NCASP). It is up to the States **to decide** whether:

- the Appropriate Authority (AA) will be also responsible for ATM security oversight e.g. in support of the NSA, or;
- ATM and Airport security oversight will remain separated (under the NSA and the AA respectively);
- a single oversight authority is responsible for all aviation security aspects (AA = NSA), or even;
- aviation security oversight, totally or partly, is carried out by a national authority other than the AA or NSA e.g. nominating a specific NSA for security or allocating some oversight functions outside the remits of the Ministry of Transport.

National Supervisory Authority				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**Security/Police/Intelligence Services**

They are responsible for providing information related to the threat (threat assessments and updates), the threat level (imminence of an attack) and advice on precautionary measures to be taken.

<b>Security/Police/Intelligence Services Points of Contact</b>				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**Critical Infrastructure Protection (CIP)**

More States nominate an authority responsible for the protection of the national infrastructure or critical infrastructure. This authority has a role to play in aviation security as well since major hubs and part of the ANS facilities may be included in the list of national critical infrastructure. In this case and according to the security alert level, special protective measures maybe taken e.g. deployment of security or military forces to protect critical assets.

Cyber security is normally part of the portfolio of these authorities; this is relevant in the light of the upcoming migration of ATM to the cyber domain (SWIM, IPv6). It should lead to declare all or part of the ATM system as critical infrastructure.

<b>Critical Infrastructure Protection</b>				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

**Airport Operators, Air Carriers, Entities (person, organisation or enterprise, other than an operator) and ANSP**

They are responsible for developing and implementing security programmes and management systems (SeMS) in order to comply with the National Civil AVSEC Programme or parts of it, for the self-protection of their aviation related systems and for providing the necessary information and support to State authorities responsible for aviation security e.g. for incident management. Those security programmes must be submitted to the responsible authority (AA and/or NSA), which may take further action if appropriate.

<b>Airport Operators, Air Carriers, Entities (person, organisation or enterprise, other than an operator) and ANSP</b>				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

It is important that regulatory, oversight and implementation functions be separated. In the case of ANS security for SES it means that the ANSP must implement a SecMS (Security Management System) to comply with Commission Implementing Regulation (EU) N° 1035/2011, and the NSA must oversight that the ANSP SecMS is compliant with the security requirements laid down in the regulation.

### Military

The role of the military is very relevant in ATM. Indeed, civil-military cooperation is an enabler for SES. Security is core to civil-military cooperation in ATM. The role of the military is multiple: regulator (MAA, Military Aviation Authorities), NSA, Airport Operator, ANSP and airspace user. The military interface with ATM security in two ways:

- for self-protection of the ATM system; providing necessary support on request of civil aviation authorities and ANSP (as per paragraph above related to Regulation N° 1035/2011) or Airports Operators for the protection of their facilities (normally in case of raised security alert levels);
- for collaborative support; defining the information and support requirements needed from ANSPs, Aircraft Operators and Airport Operators, for air defence, contingency and incident management situations.

Military focal points				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				
4				
5				

The main issue is to achieve an agreed harmonised security baseline at national level to facilitate the transition to security implementation for FAB and network level. Although aviation security remains essentially a national responsibility, the increased possibility of international threats makes a high level of cooperation among States necessary. The figure below represents a generic case of governance in aviation security and the different interdependencies at national level. States might have some differences with this model and are invited to adapt it accordingly and reflect the national ATM security organisation in Figure 11 (given as example only).

### European Aviation Crisis Coordination Cell (EACCC)

In the European Union the management of network crises is supported by the European Aviation Crisis Coordination Cell (EACCC). It consists of a representatives from the Member State holding the Presidency of the Council, the European Commission, EUROCONTROL, the Military, ANSP, airports and airspace users.

EUROCONTROL in conjunction with the EACCC members is responsible for activating and deactivating the EACCC and coordinating the management of the response to the network crisis, in accordance with the EACCC Rules of Procedure, involving close cooperation with corresponding structures in EU member States.

<b>EACCC – State Focal Point</b>				
Num.	First and last name	Title	Organisation	Contact details
1				

**National ATS Crisis Cell (NATO member States and partners)**

To meet NATO requirements, nations have agreed to establish ATS crisis cells and ATS liaison elements in the CAOCs and Airspace Coordination Centres. Airspace Coordination Centre is the Airspace Control Authority (ACA)’s primary airspace control facility for coordinating the use of airspace within the ACA’s designated airspace control area.

The National ATS crisis cells and/or ATS liaison elements are to ensure the necessary civil/military coordination for the efficient handling of changing patterns and densities of air traffic during crisis and conflict situations. Arrangements for ATS crisis cells and national implementation procedures for ATS crisis cells are detailed in NATO document Guidelines for ATM Coordination in Crisis Situation.

The activation of ATS crisis cells is one of the ATS functions in support of NATO requirements and once activated, ATS crisis cells are to ensure the responsiveness of both civil and military resources in the attainment of NATO objectives.

<b>National ATS Crisis cell</b>				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				

**CERT (Computer Emergency Response Team)**

Computer Emergency Response Teams are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficiently respond to information security incidents. They act as primary security service providers for government and citizens.

Proposal for a Directive of the European Parliament and of the Council of concerning measures to ensure a high common level of network and information security across the EU foresees that each EU member State shall set up a CERT which is responsible for handling incidents and risks according to a well-defined process.

The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process. CERT may be established within the competent authority.

<b>Computer Emergency Response Team - CERT</b>				
Num.	First and last name	Title	Organisation	Contact details
1				
2				
3				



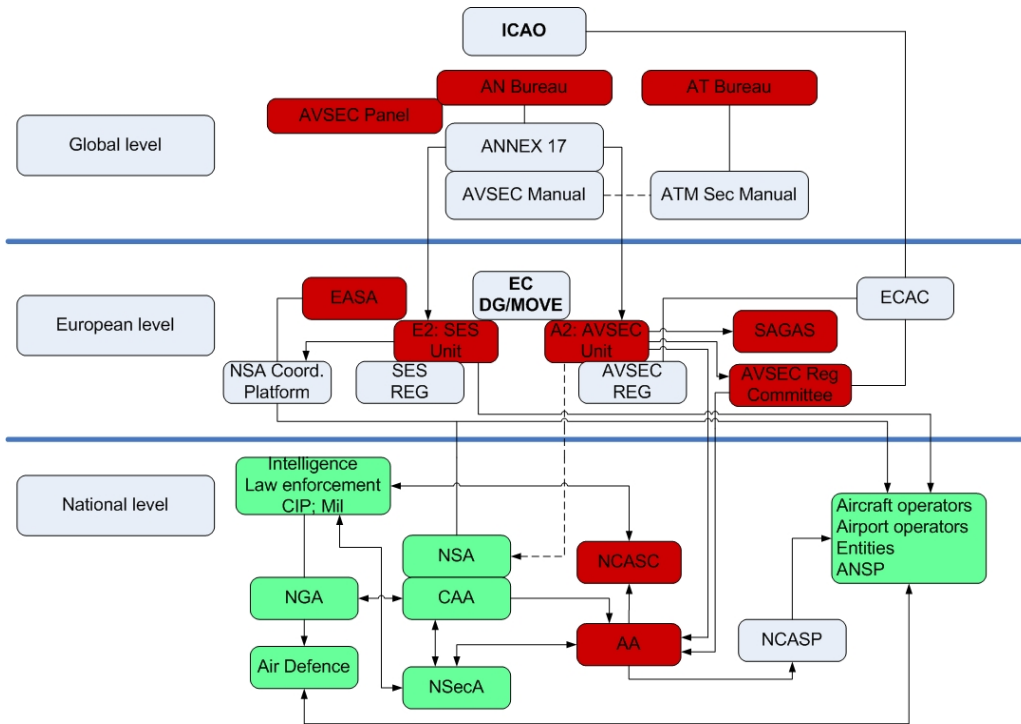


Figure 10: Governance in Aviation Security

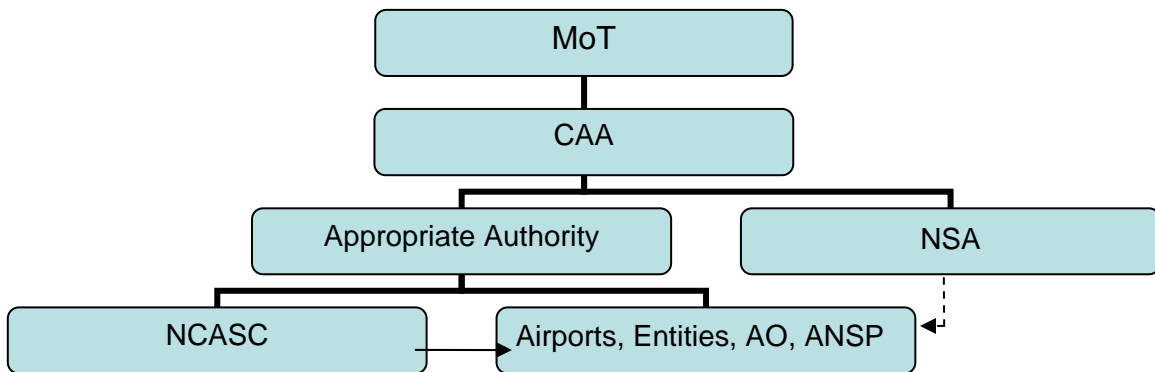


Figure 11: National ATM Security Organisation Chart

It is clear that ATM security and by extension AVSEC are not easy subjects. At national level, many persons and organisations are involved. A clear understanding of the organisation, roles and responsibilities is a must. Aviation and ATM security constitute a multi departmental and multi disciplinary subject. In a near future, this will be especially evident in the field of cyber security. Therefore, clear and effective national aviation security systems will largely facilitate the implementation of a SES security system.

# ANNEX D – Generic Guidance for Oversight of ATM Security Management Systems

## 1. ATM Security Framework

An ATM security framework is the combination in a system of organisation, means and doctrine (policies, regulations, procedures) established to protect the ATM System (people, aircraft, airspace, infrastructure and information) against attacks and acts of unlawful interference.

The basic constituents of a security framework are defined in chapters 3 to 7 of this manual:

- Scope (chapter 3)
- Policy and strategic planning (chapter 4). It includes comprehensive threat and risk assessments.
- Regulatory framework (chapter 5)
- Governance and organisation (chapter 6). It includes roles and responsibilities.
- Oversight programme (chapter 7). The oversight programme is the basic tool of the assurance framework; monitoring, inspections and audits.

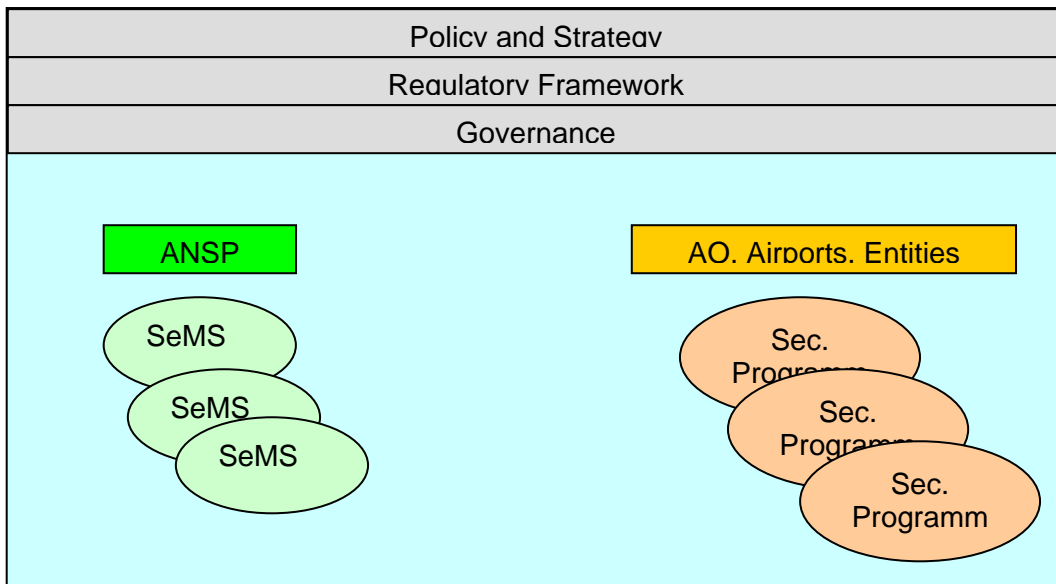
It is the **responsibility** of the national aviation and ATM security authorities to establish a national ATM security framework in support of the national aviation security programme. This framework is the reference for all involved parties e.g. ANSPs, Aircraft Operators and Airport Operators (when applicable). As part of the framework, these organisations must establish their own security programme compliant with the national programme. This obligation could be better achieved through the implementation and operation of security management systems (SeMS) (see paragraph on security management systems).

The national ATM security authorities are the **owners** of the ATM security framework while the ANSPs, aircraft operators and airport operators (when applicable) **contribute** to it by complying with the requirements of the national framework. These requirements are laid down in the international legal framework applicable to the State e.g. ICAO (Annex 17 SARPs), ECAC (Doc. 30), the EC (e.g. Regulation N°1035/2011), NATO (if the State is a member or a partner), other applicable international agreements e.g. FAB, and the national regulatory framework.

Both the Air Transport Bureau and Air Navigation Bureau are organisational units of the same international organisation, ICAO, which has clearly defined the need for a National Civil Aviation Security Programme (NCASP). ATM security is a component of the NCASP. Annex 17 describes the need for the NCASP using the word “shall” whereas a new edition of the AVSEC Manual uses the word “should”. Considering the regulatory hierarchy of ICAO Chicago Convention and its annexes, Member States shall develop a NCASP as described in Annex 17 of the Convention, including air navigation issues.

While ICAO does not strictly require the existence of SecMS, but just mention it within its guidance manual as a tool for systematically integrating security risk management, the European Union, as laid down in Commission Implementing regulation No 1035/2011, prescribes mandatory establishment of SecMS by the ANSP. The SeMS can be designed and operated together with safety and quality management systems as an integrated system.

In that context, States should be aware to develop a SecMS which is compatible with ICAO requirements for the NACSP.



**Figure 12: ATM Security Framework**

The ATM Security Framework shall ensure the achievement of the ATM Security Objective. The General Objective of ATM Security is *to determine effective mechanisms and procedures to enhance the response of ATM to security threats and events affecting flights (aircraft and passengers) or the ATM System (EUROCONTROL ATM Strategy for the Years 2000+)*.

The ATM Security Framework shall then protect the ATM System by preventing terrorist attacks and acts of unlawful interference (or any other threat) and by facilitating intervention when necessary.

The framework should address all identified ATM threats in line with the national threat assessment and security scenarios. Therefore, it should be tailored to give response to the full spectrum of security contingencies and to correct any identified ATM System security weaknesses.

The framework shall enable an ATM system robust and resilient enough to be able to cope with the full spectrum of threats. Therefore, it must be intelligence-driven and risk-based. Security risk and threat assessments have to be carried out and updated on a regular basis by the national authorities to permanently adapt the security preparedness and response to new, evolving and emerging threats.

## **2. Security Management System**

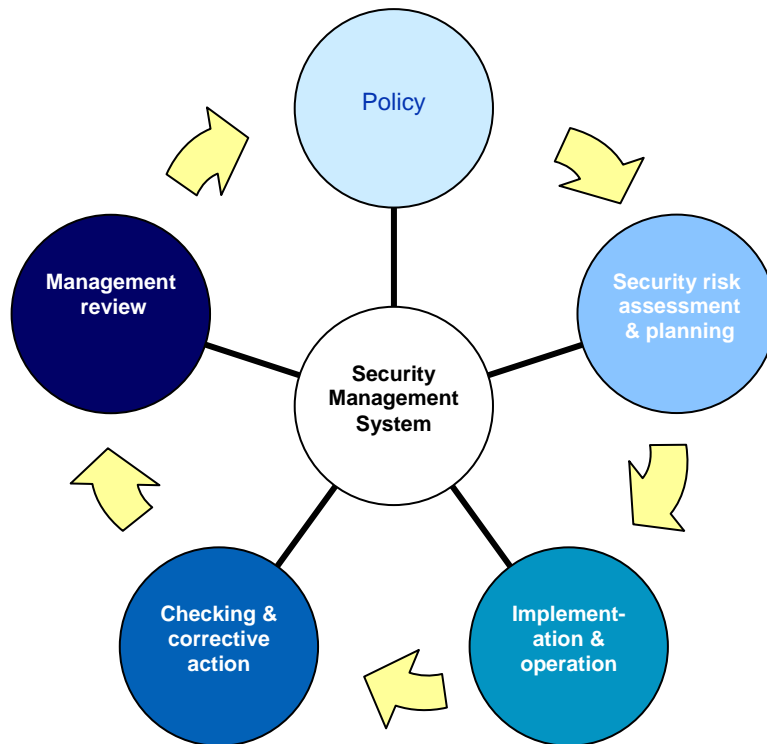
The SES regulatory framework (see chapter 5.2.1) requires air navigation service providers to establish a security management system to ensure the security of their facilities, personnel and operational data. On the other hand, NSAs are required to organise inspections and surveys to verify compliance with those requirements. It is therefore important for the NSA to have a good understanding of the notion of security management systems.

A Security Management System (SeMS) provides a framework for an organisation to assess, in a systematic manner, the security environment in which it operates, to determine if adequate preventive, responsive and contingency measures are in place, to implement and maintain security measures, and to review the ongoing effectiveness of the system.

A SeMS can be viewed as the framework within which other security activities and standards are incorporated, for example security risk assessment, identification of security measures, development of security programmes or external standards with which ATM service providers must comply.

A Security Management System (SeMS) is divided into five Key Activities:

1. Policy;
2. Security risk assessment & planning;
3. Implementation & operation;
4. Checking & corrective action;
5. Management review.



**Figure 13: Security Management Systems Overview**

These key activities are further sub-divided into 18 elements:

### **Policy**

Element 1 – Policy

### **Security Risk Assessment and Planning**

Element 2 – Security risk assessment

Element 3 – Legal, statutory, regulatory and other security requirements

Element 4 – Security management objectives

Element 5 – Security management targets

Element 6 – Security management programmes

### **Implementation and Operation**

Element 7 – Structure, authority and responsibility

Element 8 – Competence, training and awareness

Element 9 – Communication

Element 10 – Documentation and document control

Element 11 – Operational control

Element 12 – Emergency preparedness, response & recovery

### **Checking and Corrective Action**

Element 13 – Security performance measurement and monitoring

Element 14 – System evaluation

Element 15 – Failures, incidents, non-conformance and action

Element 16 – Control of records

Element 17 – Audit

### **Management Review**

Element 18 – Review and continuous improvement

Key activities and elements are designed to ensure that processes, responsibilities and expectations are clear. This framework can be used across the respective organisational levels so that individual customisation is easily possible. The framework is flexible enough to allow a variety of different management styles to be applied.

Further guidance on security management systems is provided by the EUROCONTROL Security Management Handbook (see Annex E).

### **3. Intelligence-Led, Threat-Based and Risk-Managed ATM Security**

It is a national responsibility to develop and update a threat and risk assessment for aviation to identify the threats to aviation and the related vulnerabilities to those threats (see chapter 4.8). This assessment must be shared with all involved aviation players on a need to know basis (top-down feedback). A national security assessment must be complemented with particular threat assessments carried out by the ATM organisations such as the ANSPs that provide services in that State (bottom-up feedback). States' threat assessments should be the basis to compile an agreed FAB and network threat assessment.

### **4. Practical ATM Security Oversight**

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

This can be done through the establishment of an inspection and audit programme. Inspections examine the implementation of relevant national civil aviation security programme requirements by an airline, ANSP, airport or other entity involved in security. Audits are an in-depth compliance examination of all aspects of the implementation of the national civil aviation security programme (see annex on Definitions). Nevertheless, both inspection and audits must not restrict themselves to compliance verification (**prescription-based**) but go beyond the regulatory compliance and concern the system-based and **outcome-oriented** aspects.

#### **4.1 Security Oversight Process**

A generic security oversight process is described in the figure below.

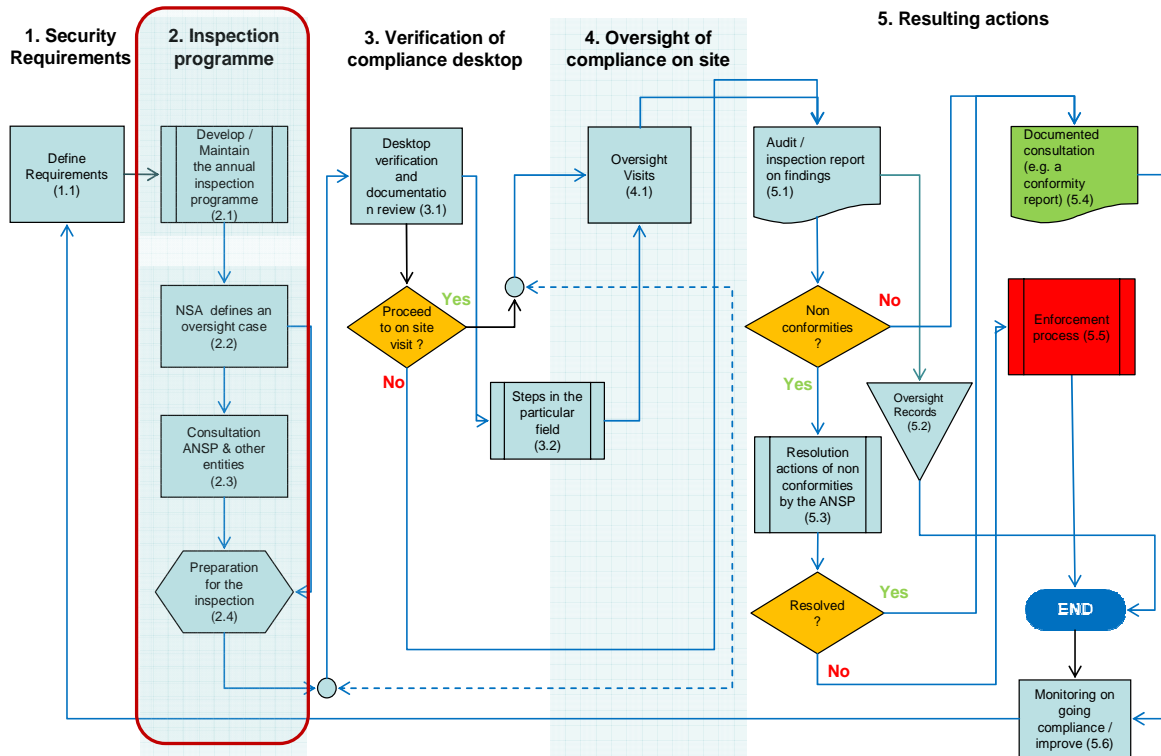


Figure 14: Generic Security Oversight Process

#### 4.2 Security Oversight Documentation Management

The practical oversight is facilitated by proper documentation generation and management (see table below). A main part of it is the definition of security checklists and questionnaires, following a top-down process starting with the **identification of the security requirements** (see paragraph above). Most security requirements stem from the regulatory framework (global, regional and national). Security requirements and check lists are described in the appendixes to this annex.



Requirement	Expectation	Means of compliance	Evidence	Detailed requirements (questionnaire)	Assessment	Way ahead
As laid down in the regulation/legislation or applicable directive or standard	Of the oversight authority on how the inspected entities must fulfil the requirement . It must be communicated to the entities.	Arguments claiming to fulfil the expectation , provided by the inspected entities and agreed by the oversight authority	To justify the arguments; provided by the inspected entities and assessed by the oversight authority	Used by the inspectors (normally shared, partly - not all - with the inspected entity)	By the inspectors (coordinated as much as possible with the inspected entity)	Corrective actions/conclusions (coordinated as much as possible with the inspected entity)

**Table 2: Security Oversight Documentation Process**

**4.3 Assessing the Current Situation**

Before developing and implementing an ATM security oversight plan, it is very important for national authorities to have an indication of the current status of compliance and maturity within the State. Self-assessment questionnaires are an efficient tool to obtain this baseline and benchmarking information. Different self-assessments questionnaires are included in the Appendix 1 to this Annex.

**4.4 The oversight Plan**

Finally, once the baseline status of ATM security within the State is well known by the authorities, an oversight plan can be much better developed and implemented. Guidance and a lay out of an ATM security oversight programme are provided in Appendix 4.

**4.5 Security Questionnaires**

In order to support the security oversight function by the national authorities, security questionnaires must be issued. Examples of such questionnaires are provided in Appendix 2 (oversight of SeMS) and 3 (specific for INFOSEC). The questionnaires must be complemented with national input derived from specific national legislation applicable to ATM.

**Appendix 1: Self-Assessment Questionnaires**

**QUESTIONNAIRE ON ATM SECURITY IMPLEMENTATION STATUS FOR NSAs**

(The questionnaire, once filled in, shall be classified as Restricted and subject to applicable national protective measures)

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On going	N	
R1: Holistic approach: ATM Security embedded into the National AVSEC Programme	(as per ICAO Annex 17, amendment 12 <sup>th</sup> , Chapter 3.5: Each Contracting State <b>shall</b> require <b>air traffic service providers</b> operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State)	ATM security is part of the overall national AVSEC programme, including quality control and training programmes Harmonised national ATM security systems are integrated in the national AVSEC system	National AVSEC Programme and its constituents	1. National AVSEC Authority (Appropriate Authority) nominated				
				2. National AVSEC Committee (NCASC) established (ToR)				
				3. The ATM players, e.g. ANSP and aircraft operators (AO) participate in the NCASC				
				4. National AVSEC programme (NCASP), approved by the competent authority and implemented, including: a) Organisation b) Policies/framework c) quality control programme d) training programme				
				5. Security Programmes for AO and ANSP are issued and endorsed by the AA as part of the overall				

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
				accreditation/designation process				
R2: Security Oversight	<ul style="list-style-type: none"> <li>- ICAO Annex 17, chapter 3.4</li> <li>- EC 550/2004; role of NSAs (inspections and surveys)</li> <li>- ECAC Doc. 30, Chapter 13 (ATM Security)</li> <li>- EC 300/2008; national AVSEC quality control programme</li> </ul>	<ul style="list-style-type: none"> <li>- Oversight function is executed as part of the AVSEC Programme/Quality control programme</li> <li>- Separation between oversight function, regulatory function and service provision</li> </ul>	National AVSEC Programme and its constituents (quality control programme)	1. Security oversight plan as part of the Quality control programme				
				2. Clear roles and responsibilities are defined in the AVSEC Programme				
				3. ANSP Audits/inspections reports				
				4. Aircraft operators Audits/inspections reports				
R3: Comprehensive ATM security/holistic approach	<ul style="list-style-type: none"> <li>- ICAO ATM Security Guidance<sup>11</sup></li> <li>- ECAC Doc. 30 (Chapter 13)</li> </ul>	ATM Security key areas; <ul style="list-style-type: none"> <li>- Self Protection and Collaborative Support to national civil and military authorities</li> </ul> are addressed by the AVSEC programme The national regulatory framework includes specific legislation for airspace security/support to NGA ATM support to national and international security and defence requirements is fully recognised and	National AVSEC Programme and its constituents (ATM security and its 2 key areas)	1. Documented parts of the AVSEC Programme addressing both the self protection and the collaborative support ATM security areas				
				2. Comprehensive composition of the AVSEC committee (NCASC), e.g. airlines, ANSP and military participate				
				3. ANSP security programmes or SeMS approved and implemented				

<sup>11</sup> The Guidance is expected to be published by the end of 2012

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
		integrated in the NCASP and associated SeMS and security programmes, including interface with airspace security, in line with national and international requirements		4. Aircraft operators Security Programmes or SeMS approved and implemented 5. Documented specific legislation for airspace security/support to NGA				
R4: Cyber security	- ICAO Annex 17, 12 <sup>th</sup> amendment, chapter 4.9, and it AVSEC Manual (Chapter 18) - ECAC Doc. 30 (Chapter 14 <sup>th</sup> ) - EC 1035/2011 - EC 73/2010	Cyber security issues are part of the overall AVSEC activities	National AVSEC Programme and its constituents (cyber security programme)	1. Cyber security is part of the AVSEC Programme, included oversight and training				
				2. Cyber security is part of the threat and risk assessment plan				
				3. threat and risk assessment reports				
				4. ANSP, AO and other entities audits/inspection reports				
R5: Security is intelligence driven, threat based and Risk managed	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition - ICAO ATM Security Guidance - EC 1035/2011	AVSEC activities are based on continuous threat and risk assessments, with support from the national security and intelligence organisations Security is monitored and improved based on lessons learnt	National AVSEC Programme and its constituents (Threat and Risk Assessments, security monitoring and improvement)	1. National AVSEC Threat and Risk assessment plan is part of the AVSEC Programme				
				2. Threat and Risk assessment studies carried out. National threat assessments are available and are used to carry out local security threat and risk assessments, which are updated on a regular basis				

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
				3. Security monitoring system, Lessons learnt and mitigation actions implemented				
R6: Incident and Crisis management, contingency planning	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition - ICAO ATM Security Guidance - EC 1035/2011	- The management of security incidents and crisis is fully addressed by the National AVSEC Programme, at organisational and procedural level - Contingency planning is part of the National AVSEC Programme	National AVSEC Programme and its constituents (incident/crisis management system, contingency plans for ATM)	1. There is a system established, including procedures, for incident management (e.g. airspace security incidents). The system is regularly exercised and updated with lessons learnt				
				2. There is an aviation crisis management system established, which interfaces with the national crisis management organisations and the EACCC (European Aviation Crisis Coordination Cell in the Network Manager). The system is regularly exercised and updated with lessons learnt				
				3. National aviation and ATM security Contingency Plans have been developed and approved by the Appropriate Authority. They cater for both pre-defined and 'unknown' scenarios. The plans are regularly exercised and updated with lessons learnt				

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
				4. As part of the security management systems of ANSP and other concerned organisations, there is a system in place for security breach detection, incident notification, lessons learnt and implementation of corrective measures				
				5. As part of the security management systems of ANSP and other concerned organisations, there are contingency and crisis management plans approved and implemented. The plans are regularly exercised and updated with lessons learnt.				
R7: Training	<ul style="list-style-type: none"> <li>- ICAO Annex 17, chapter 3.1</li> <li>- ICAO AVSEC Manual, 8<sup>th</sup> Edition, Chapter 8</li> </ul>	<ul style="list-style-type: none"> <li>- the ATM Security training function is executed as part of the AVSEC Programme, within the National Civil Aviation Security Training Programme (NCASTP)</li> </ul>	<ul style="list-style-type: none"> <li>- National AVSEC Programme and its constituents, i.e. National Civil Aviation Security Training Programme (NCASTP)</li> </ul>	1. ATM security training chapter within the NCASTP				
				2. ATM security training needs and requirements identified in the NCASTP: security culture, education, awareness, training and exercise plan, qualifications, training centres, etc				
				3. Clear roles and responsibilities for ATM security training established				

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
				4. ATM security training includes both self protection and collaborative support aspects				
R8: Safety/Security Interface	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition, Chapter 9 - EC 1035/2011	Security management is integrated or at least coordinated and aligned with safety management (and ideally with other management systems, e.g. Quality), in order to exploit synergies, avoid overlaps and make sure that security developments do not jeopardise safety and vice versa	- National AVSEC Programme and its constituents (Safety and security interface definition) - Documented process of Safety/security (and ideally quality) integration, coordination and alignment, included in security programmes of ANSP, AO and other applicable entities	1. Risk Management processes consider all hazard approach				
				2. Risk management is exercised at highest level (national, e.g. NCASC and board corporate for AO and ANSP)				
				3. Safety and security managers coordination meetings				
				4. Joint complementary multidisciplinary audits inspections				
				5. Integrated security/safety (and ideally quality) management systems for ANSP, AO and other applicable entities				
R9: Security Information Exchange	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition, Chapter 4	National security activities are based on continuous sharing of security information, like threat and	Federated collaborative security information exchange mechanism, for mutual	1. Security information and Threat and Risk assessments are shared within the State ATM security partners				

REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE SELF-ASSESSMENT			RMKS (e.g. issues encountered, corrective actions, completion dates, etc.)
					Y	On	N going	
		risk assessments, with support from the national security and intelligence organisations. Bilateral and regional agreements are in place, including provisions for the protection of classified and sensitive information	support : - within the State - with neighbouring and other States including provisions for the protection of classified and sensitive information	2. Security information and Threat and Risk assessments are shared with neighbouring and other States  3. Intelligence inputs are provided to established the Threat level Security alerts  4. Security incidents; post incident analysis and reports; lesson learnt  5. A point of contact network is established for dissemination of security information  6. Documented nomination and job description of security officers for the protection of classified information, and its rules of procedure				
R10: International collaboration	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition, Chapter 3 and 4	The NCASP caters for bi-lateral, multi-lateral and regional security agreements in order to improve and harmonise global security and facilitate cross-border arrangements and handling of incidents	Bi-lateral, multi-lateral and regional security agreements established.	1. Documented bi-lateral, multi-lateral and regional security agreements are in place and exercised  2. Cross-border arrangements with neighbouring (FAB) States are documented and exercised  3. Provisions of international agreements are documented in the NCASP and included in its associated elements, i.e. NCASP, NCASQCP (Quality Control Programme)				



**QUESTIONNAIRE ON REGULATORY GAP ANALYSIS REGARDING THE SES AND NATIONAL LEGISLATION**

(The questionnaire, once filled in, shall be classified as Restricted and subject to applicable national protective measures)

REGULATION	NAME	SECURITY ASPECT	IS THE CURRENT REGULATORY FRAMEWORK SUFFICIENT TO ADDRESS ATM SECURITY? COULD IT BE IMPROVED AND HOW?
EC 550/2004	ANS Provision Regulation, establishing common requirements for the safe and efficient provision of ANS in the Community	Includes the obligation of the national supervisory authorities (NSA) to organise inspections and surveys to verify compliance with the requirements (laid down in EC Reg. N° 1035/2011)	
EC 1035/2011	Laying down common requirements for the provision of air navigation services	<p>An air navigation service provider shall establish a security management system to ensure:</p> <ul style="list-style-type: none"> <li>(a) the security of its facilities and personnel so as to prevent unlawful interference with the provision of services;</li> <li>(b) the security of operational data it receives or produces or otherwise employs so that access to it is restricted only to those authorised.</li> </ul> <p>The security management system shall define:</p> <ul style="list-style-type: none"> <li>(a) the procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;</li> <li>(b) the means designed to detect security breaches and to alert personnel with appropriate security warnings;</li> <li>(c) the means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.</li> </ul> <p>An air navigation service provider shall ensure the security clearance of its personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data.</p> <p>At the latest one year after certification, an air navigation service provider shall have in place contingency plans for all the services it provides in the case of events which result in significant degradation or interruption of its services.</p> <p>'A provider of aeronautical information services shall ensure the <b>integrity of data</b> and confirm the level of accuracy of the</p>	

REGULATION	NAME	SECURITY ASPECT	IS THE CURRENT REGULATORY FRAMEWORK SUFFICIENT TO ADDRESS ATM SECURITY? COULD IT BE IMPROVED AND HOW?
		<p>information distributed for operations, including the source of such information, before such information is distributed'.            'A provider of communication, navigation or surveillance services shall ensure the <b>availability</b>, continuity, accuracy and <b>integrity</b> of its services'</p>	
EC 73/2010	laying down requirements on the quality of aeronautical data and aeronautical information for the Single European Sky	<p>Lays down the requirements on the quality of aeronautical data and aeronautical information in terms of accuracy, resolution and <b>integrity</b>.</p> <p>List Security management objectives:</p> <ul style="list-style-type: none"> <li>- to <b>ensure the security of aeronautical data</b> and aeronautical information received, produced or otherwise employed so that it is protected from interference and access to it is restricted only to those authorised;</li> <li>- to ensure that the security management measures of an organisation meet appropriate national or international requirements for critical infrastructure and business continuity, and international standards for security management, including the ISO standards referred to hereafter;</li> </ul> <p>Regarding the ISO standards, the relevant certificate issued by an appropriately accredited organisation, shall be considered as a sufficient means of compliance.</p> <p>ISO referred to:</p> <ul style="list-style-type: none"> <li>- International Organisation for Standardisation, ISO/IEC 17799:2005<sup>12</sup> — Information technology — Security techniques — Code of practice for information security management (Edition 2 — 10.6.2005).</li> <li>- International Organisation for Standardisation, ISO 28000:2007: — Specification for security management systems for the supply chain (Edition 1 — 21.9.2007 under</li> </ul>	

<sup>12</sup> The current name of the standard is ISO 27002

REGULATION	NAME	SECURITY ASPECT	IS THE CURRENT REGULATORY FRAMEWORK SUFFICIENT TO ADDRESS ATM SECURITY? COULD IT BE IMPROVED AND HOW?
		revision, to be replaced by Edition 2 target date 31.1.2008 [At enquiry stage]	
EC 300/2008	Common rules in the field of civil aviation security	<p>Includes requirements for: Common <b>basic standards</b> for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation. Most of these common standards refer to security on the ground. However, there are also '<b>IN-FLIGHT SECURITY MEASURES</b>', namely:</p> <ol style="list-style-type: none"> <li>1. Without prejudice to the applicable aviation safety rules: <ol style="list-style-type: none"> <li>(a) unauthorised persons shall be prevented from entering the flight crew compartment during a flight;</li> <li>(b) potentially disruptive passengers shall be subjected to appropriate security measures during a flight.</li> </ol> </li> <li>2. Appropriate security measures such as training of flight crew and cabin staff shall be taken to prevent acts of unlawful interference during a flight.</li> <li>3. Weapons, with the exception of those carried in the hold, shall not be carried on board an aircraft unless the required security conditions in accordance with national laws have been fulfilled and authorisation has been given by the states involved.</li> </ol>	

<p align="center"><b>National Regulatory Framework</b>                      (e.g. National regulations for Aviation Security, ATM Security, Airspace Security/support to NGAs, etc.)</p>					
Num.	Rank (e.g. Law, Decree, regulation...)	Title	Subject/Content extract	Relevant aspects	Assessment (Is the current regulatory framework sufficient to address ATM security? Could it be improved? How?)
1					
2					
3					
4					
5					

**QUESTIONNAIRES FOR FABS****ATM Security Implementation Status at FABS**

(The questionnaire, once filled in, shall be classified as Restricted and subject to applicable national protective measures)

<b>REQUIREMENT</b>	<b>EXPECTATIONS</b>	<b>EVIDENCE</b>	<b>SELF-ASSESSMENT</b>
FAB must support national security and defence i.e. airspace security and national civil aviation security programme of FAB States	ATM Security is included in the FAB Agreement as part of the mutual responsibilities in support of national security and defence policies. FAB ATM security provisions cater for both self-protection of the ATM system and ATM collaborative support to national civil and military authorities. Must include provisions for crisis management and contingency situations.	1. FAB ATM Security Framework (SeMS), as part of the FAB Agreement, approved by the competent authorities and implemented, including: a) Organisation b) Policies c) Roles and responsibilities d) Mutual assistance i.e. contingency/ crisis management e) quality control agreements/ arrangements f) training agreements/arrangements g) security information exchange	1. Yes/No/Comments  a) Yes/No/Comments b) Yes/No/Comments c) Yes/No/Comments d) Yes/No/Comments  e) Yes/No/Comments  f) Yes/No/Comments g) Yes/No/Comments
Agreed security policies, standards and practices	1. Mutual recognition of the SeMS of FAB ANSP 2. Harmonised security policies and standards i.e. for vetting	1. FAB Agreement 2. Letter of mutual recognition	1. Yes/No/Comments  2. Yes/No/Comments
Security Oversight	1. Mutual recognition of security oversight functions 2. Oversight function is executed as part of the quality control programme of the FAB agreement 3. Joint audit teams are established 4. Oversight function is separated from the regulatory function	1. FAB Agreement 2. FAB Security oversight plan as part of the FAB Quality control arrangement/programme 3. Clear roles and responsibilities are defined in the FAB security framework agreement 4. FAB ANSP audits/inspection reports	1. Yes/No/Comments  2. Yes/No/Comments  3. Yes/No/Comments 4. Yes/No/Comments
Harmonised training requirements	1. Mutual recognition of security training programmes 2. Mutual recognition of security training qualifications and certificates 3. Cross-training agreements/arrangements	1. FAB Agreement 2. FAB Security training arrangements as part of the FAB security framework agreement	1. Yes/No/Comments  2. Yes/No/Comments 3. Yes/No/Comments
Harmonised airspace security	Harmonised ASSIM arrangements and procedures (RENEGADE, COMLOSS, bomb on	1. FAB Agreement 2. FAB Security Framework agreement	1. Yes/No/Comments 2. Yes/No/Comments

REQUIREMENT	EXPECTATIONS	EVIDENCE	SELF-ASSESSMENT
Incident management (ASSIM), including High Seas security arrangements	board, hijack) including when in High Seas Mutual assistance and support for crisis management and contingency situations	3. FAB security arrangements for High Seas security incident management 4. FAB arrangements for contingency planning and crisis management	3. Yes/No/Comments 4. Yes/No/Comments
Cyber security	Cyber security issues are part of the overall FAB security management activities FAB INFOSEC environment implemented	1. Cyber security is part of the FAB security framework, including INFOSEC oversight and training 2. FAB threat and risk assessment reports 3. ANSP audits/inspection report	1. Yes/No/Comments 2. Yes/No/Comments 3. Yes/No/Comments
Security Information Exchange	Federated collaborative security information exchange mechanism for mutual support: <ul style="list-style-type: none"> <li>- Threat and Risk assessment</li> <li>- Threat level</li> <li>- Intelligence input</li> <li>- Security alerts</li> <li>- Security incidents</li> <li>- Post incident analysis and reports</li> <li>- Lesson learnt</li> <li>- Etc.</li> </ul> FAB security activities are based on continuous shared threat and risk assessments, with support from national security and intelligence organisations	1. FAB Agreement 2. FAB Security Framework agreement 3. FAB security information exchange agreement 4. FAB threat and risk assessment reports	1. Yes/No/Comments 2. Yes/No/Comments 3. Yes/No/Comments 4. Yes/No/Comments

**Regulatory Gap Analysis for FABs**

(The questionnaire, once filled in, shall be classified as Restricted and subject to applicable national protective measures)

REGULATION	NAME	SECURITY ASPECT	IS THE CURRENT REGULATORY FRAMEWORK SUFFICIENT TO ADDRESS ATM SECURITY? COULD IT BE IMPROVED AND HOW?
EC 176/2011	on the information to be provided before the establishment and modification of a functional airspace block	<p><b>Does not include security requirements</b></p> <p>In the justification material it is stated that 'the draft IR does not elaborate requirements on the issue of security on the basis that security is addressed in the SES basic regulations (as amended). It was concluded that security issues may therefore per se be a justification not to provide certain information. Security was considered in the context of:</p> <ul style="list-style-type: none"> <li>• ANSP security issues (ATM security), and</li> <li>• national security and defence issues'</li> </ul>	
EUROCONTROL Guidelines regarding EC 176/2011	Guidelines on Generic Military Requirements to be considered when establishing or modifying a Functional Airspace Block	<p>Within the Guidelines, there are principles and requirements on governance, defence, civil-military cooperation and security i.e.:</p> <ul style="list-style-type: none"> <li>• The ATM system shall take the necessary protective measures to minimise the effectiveness of hostile acts against ATM facilities, systems and data;</li> <li>• As far as possible, FAB States will strive for homogeneity of security and defence policies;</li> <li>• The international dimension imposes the harmonised and effective application of suitable security measures such as RENEGADE.</li> </ul>	
EC. 2096/2005	Laying down common requirements for the provision of air navigation services	Annex I, General requirements/Security; paragraph about security requirements stating: <i>An air navigation service provider shall ensure the security clearance of its personnel, if appropriate, and <b>coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data</b></i>	
EC 550/2004	ANS Provision Regulation establishing common requirements for the safe and efficient provision of ANS in the Community	Article 11, Relations with military authorities; Member States shall, within the context of the common transport policy, take the necessary steps to ensure that <b>written agreements</b> between the competent civil and military authorities or equivalent legal arrangements are established in respect of the management of specific <b>airspace blocks</b> .	
Applicable, if any, national regulatory framework must be added (see bottom of questionnaire in Appendix 1)			

## **QUESTIONNAIRE ON COST AND BENEFITS OF SECURITY (NSAS, ANSPS)**

(The questionnaire, once filled in, shall be classified as Restricted and subject to applicable national protective measures)

1. After entry into force of security regulations, has your organisation made any investment to comply with the regulation (i.e. recruitment of security experts, upgrades of security systems, training needs, awareness campaigns, etc.)?
2. Has your organisation realised benefits from implementing security? e.g. increase awareness, better asset control (e.g. less theft, less misuse of ICT systems), better incident management e.g. increased reporting of abnormal situations and cooperation from all staff (security, as safety, is everybody's responsibility and part of corporate business), contribution to staff management (e.g. absence control, improved access control; visitors, suppliers); improvement in working environment/conditions; synergies with safety and facility managers (as efficiency factor and cost saving factor).



Regulation	Description	Cost Aspects	Benefit Aspects (items in question 2 above are provided as reference)	Remarks
EC 550/2004	ANS Provision Regulation establishing common requirements for the safe and efficient provision of ANS in the Community	<ul style="list-style-type: none"> <li>- Recruitment</li> <li>- Training</li> <li>- Awareness</li> <li>- Investments (new security systems, upgrades)</li> <li>- Others (please specify)</li> </ul>		
EC 1035/2011	Laying down common requirements for the provision of air navigation services	<ul style="list-style-type: none"> <li>- Recruitment</li> <li>- Training</li> <li>- Awareness</li> <li>- Investments (new security systems, upgrades)</li> <li>- Others (please specify)</li> </ul>		
EC 73/2010	Laying down requirements on the quality of aeronautical data and aeronautical information for the Single European Sky	<ul style="list-style-type: none"> <li>- Recruitment</li> <li>- Training</li> <li>- Awareness</li> <li>- Investments (new security systems, upgrades)</li> <li>- Others (please specify)</li> </ul>		
EC 300/2008	Common rules in the field of civil aviation security	<ul style="list-style-type: none"> <li>- Recruitment</li> <li>- Training</li> <li>- Awareness</li> <li>- Investments (new security systems, upgrades)</li> <li>- Others (please specify)</li> </ul>		

**Appendix 2: Questionnaire on Oversight of Security Management Systems and Security Programmes**

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y	On	N Going	
1	System approach/ATM security system	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, Chapter 9</li> <li>- EC 1035/2011, Annex 1, Paragraph 4</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	Security processes are integrated in a security management system (SeMS) The SeMS could be part of an integrated corporate management system including other systems, like safety and quality	National AVSEC Programme and its constituents; SeMS and Security Programmes for ANSP. AO and other entities are issued and approved in the context of and compliant with the NCASP	1. Documented SeMS delivered and endorsed by the AA as part of the overall accreditation/designation process				
					2. The SeMS, approved by the competent authority, are implemented, including: <ul style="list-style-type: none"> <li>h) Organisation</li> <li>i) Policies/framework</li> <li>j) Security Plans</li> <li>k) quality control programme</li> <li>l) training programme</li> </ul> <b>consistent</b> with the provisions of the NCASP				
2	Security Policy	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, Chapter 2</li> <li>- ECAC Doc. 30, Annex IV-13-A</li> </ul>	The national security policy as laid down in the NCASP is fully embedded into the organisation	Corporate security policy statement or document	1. Documented corporate security policy which fully reflects the national security policy as per the NCASP				
					2. Education, awareness and training material confirming that the policy is communicated, disseminated, briefed,				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
					known and applied by all staff				
3	Asset <sup>13</sup> Management	- ECAC Doc. 30, Chapter 13	The organisation has complete knowledge of its own assets, the environment in which it operates and the critical aspects that could impede the delivery of its service	A documented process addressing Asset Management	<p>1. Documented description of the organisation, its operations (internal and outsourced), its assets and their ownership, and any other aspect relevant to the maintenance of adequate security. Assets should include information assets and their classification.</p> <p>2. All assets of the organisation are identified and classified in 2 categories:                      - <b>Primary Asset</b>                      Intangible function, service, process or information that are part of the ATM system within the scope of the organisation and has value to the system                      - <b>Supporting Asset</b></p>				<p><b>Asset:</b> Elements in the system that has value for the achievement of business objectives</p> <p>The supporting assets might be broken down into critical levels, if required</p>

<sup>13</sup> According to ECAC Doc. 30, the term 'assets' includes ATM/CNS infrastructures, facilities and systems

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
					Entities which enable the primary assets. Supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets				
4	Human Resources Security	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, Chapter 7</li> <li>- EC 1035/2011, Annex 1, Paragraph 4</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	The organisation has a clear policy and requirements for the selection, recruitment and training of personnel. The policy is compliant with applicable national regulations and other provisions laid down in the NCASP.	A documented process addressing Human Resources Security	<ol style="list-style-type: none"> <li>1. Documented activities describing the security screening, selection, education, awareness and training process for all employees, contractors and other personnel, to ensure that they all meet their security responsibilities and requirements</li> <li>2. Nomination by the senior corporate manager of a security officer responsible for the activities in point 1 above and the security clearances of staff. This nomination and its job description is</li> </ol>				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
					<p>communicated to all staff. (This security officer can be the same as the person described in bullet 14 for protection of information)</p>				
					<p>3. Documented process on recruitment security requirements: list of background checks or security clearances, catalogue of post requiring security clearances, confidentiality measures, forms and point of contact within the national security authority</p>				
					<p>4. Documented process and responsibilities, in case of external organisations are used for security provision</p>				
5	Security assurance, oversight and	- ICAO Annex 17, chapter 3.4	The organisation follows up the	Documented security oversight and	1. Audits and inspection reports (external and internal)				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y   On   N Going			
	monitoring	<ul style="list-style-type: none"> <li>- EC 550/2004; role of NSAs (inspections and surveys)</li> <li>- EC 300/2008; national AVSEC quality control programme</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	<p>results of internal and external audits and inspections and implements the recommendations and corrective measures identified in the reports</p>	<p>monitoring plan Internal ATM security oversight system</p>	<p>2. Action plans resulting from inspections and reports</p> <p>3. Updated audit and inspection programmes (both external form the authorities and internal from the organisation)</p> <p>4. The internal ATM security oversight system agreed by the NSA includes:</p> <ul style="list-style-type: none"> <li>- Policy, derived from the NSA policy</li> <li>- Objectives</li> <li>- Oversight plan</li> <li>- Oversight training and qualifications; ATM security auditors</li> <li>- Recognition scheme agreed by the NSA</li> <li>- Documentation: questionnaires, means of compliance, support and guidance</li> </ul>				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
					material, etc.				
6	Comprehensive ATM security/holistic approach	<ul style="list-style-type: none"> <li>- ICAO ATM Security Guidance<sup>14</sup></li> <li>- ECAC Doc. 30 (Chapter 13)</li> </ul>	<p>ATM Security key areas;</p> <ul style="list-style-type: none"> <li>- Self-protection and</li> <li>- Collaborative support to aviation security and national security and defence</li> </ul> <p>are addressed by the organisation's SeMS</p> <p>Agreed common understanding of ATM security, its two components (self-protection and collaborative support to State authorities) exist in the organisation Security</p>	<p>SeMS and its constituents i.e. self-protection measures and collaborative support to National Authorities measures</p>	<ol style="list-style-type: none"> <li>1. Documented security measures and procedures for resilience/self protection of the organisation</li> <li>2. Documented security measures and procedures for collaborative support to National Authorities e.g. airspace security incident management, hijack/Renegade, COMLOSS procedures, etc</li> <li>3. The SeMS includes interfaces with other security players e.g. airlines, airports, CNS providers, in support of aviation security (e.g. laser attacks, hijacks, CNS jamming, etc.)</li> </ol>				

<sup>14</sup> The Guidance is expected to be published by the end of 2012

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
			measures for both areas are implemented and integrated in the SecMS.						
7	Cyber security <sup>15</sup>	<ul style="list-style-type: none"> <li>- ICAO Annex 17, 12<sup>th</sup> amendment, chapter 4.9, and it AVSEC Manual (Chapter 18)</li> <li>- ECAC Doc. 30 (Chapter 14<sup>th</sup>)</li> <li>- EC 1035/2011, Annex I, Paragraph 4 (security and contingency plans), and Annex III (specific requirements for the</li> </ul>	Cyber security issues are part of the overall security activities of the organisation and fully addressed within the SeMS	SeMS and its constituents i.e. self-protection measures/cyber security and resilience measures Commission Regulation (EU) N° 73/2010 Considers <u>sufficient means of compliance</u> against its requirements, the following: <ul style="list-style-type: none"> <li>- ISO 27000 family</li> </ul>	<ol style="list-style-type: none"> <li>1. Documented cyber security provisions within the SeMS, including oversight and training, and follow up of actions from audits/inspection reports</li> <li>2. A documented process addressing the protection of <u>operational data</u><sup>16</sup> in order to guarantee its confidentiality, integrity and availability and ensure the correct and secure operation of communications and information systems and</li> </ol>				

<sup>15</sup> A specific more detailed questionnaire regarding cyber security is provided in Appendix 3



#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y	On	N	Going
		provision of meteorological services), Annex IV (specific requirements for the provision of aeronautical information services and Annex V (specific requirements for the provision of communication, navigation or surveillance services) - EC 73/2010 (laying down requirements on the quality of aeronautical data and aeronautical information		(27001 and 27002) Information technology /security techniques /code of practice for information security management - ISO 28000:2007, specification for security management systems for the supply chain	processes, including connectivity with third parties  3. Documented process to ensure the availability, continuity, accuracy and integrity of CNS services, and confirmation of the quality level of the services e.g. demonstration that the equipment is regularly maintained and where required calibrated  4. Documented process ensuring the availability, integrity, confidentiality and accuracy of aeronautical information and data (including checking the source of such information) in a suitable form for flight operations and provision of air traffic services				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
		for the single European sky)			5. Documented process ensuring the availability and accuracy of meteorological information (including checking the source of such information), in a suitable form for flight operations, provision of air traffic services, search and rescue and aerodromes				
					6. Documented roles and responsibilities for cyber security within the organisation				
					7. Cyber security is part of the threat and risk assessment plan: threat and risk assessment reports include cyber threats				
					8. Documented Information Systems life cycle security; acquisition, development and				

<sup>16</sup> A definition of operational data is provided by Regulation (EC) N° 549/2004 laying down the framework for the creation of the Single European Sky (the Framework Regulation): ‘operational data’ means information concerning all phases of flight that are required to take operational decisions by air navigation service providers, airspace users, airport operators and other actors involved.

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
					maintenance and 3. 3. Decommissioning, to ensure that security is an integral part of information systems during all phases of design, development, testing, implementation and maintenance and decommissioning (i.e. making sure information is erased before giving away IT systems)				
8	Security is intelligence-driven, threat-based and risk-managed	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, 8<sup>th</sup> Edition</li> <li>- ICAO ATM Security Guidance</li> <li>- EC 1035/2011</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	The organisation carries out continuous threat, vulnerability and risk assessments in line with the NCASP, with support from national security and intelligence organisations Security is	Documented SeMS and its constituents (threat, vulnerability and risk assessments, security monitoring and improvement, consistent with the provisions in the NCASP) A documented	1. Documented threat , vulnerability and risk assessment studies and reports carried out by the organisation				
					2. Documented exchange of security information with national authorities within the NCASC, e.g. intelligence and security organisations				
					3. Documented security monitoring system, and examples of lessons learnt and mitigation actions implemented				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
			<p>monitored and improved based on risk assessments results and lessons learnt. Proper <u>risk</u> assessments must be carried out. The <u>threat</u> assessment is just a part of the risk assessment. The threat is usually difficult to grasp, because it may change very suddenly, for example because new capacity is acquired or because there has been a change in intention due to incidents or radicalization. The threat actors will also do whatever</p>	<p>process addressing the risk assessment and treatment; to identify, quantify and prioritise threats and risks against criteria and objectives relevant to the organisation and the appropriate controls to reduce the risk</p>	<p>4. Comprehensive, regularly updated, threat register based on threat assessments, threat watch, evolution and monitoring</p>				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y	On	N Going	
			<p>they can to develop new methods. A more constant factor within the risk assessment is the <u>vulnerabilities</u>. The most important object of analysis should be the vulnerabilities of the <u>most critical</u> assets within the organization. The main goal should be to reduce the vulnerabilities of these assets, thereby reducing the overall risk. The threat should be taken into account to provide examples of modus</p>						

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
			operandi, etc						
9	Incident and crisis management, contingency planning and critical infrastructure	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, 8<sup>th</sup> Edition, Chapter 17</li> <li>- ICAO ATM Security Guidance</li> <li>- EC 1035/2011</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	The management of security incidents and crisis is fully addressed by the SeMS of the organisation, at organisational and procedural level Crisis management and contingency planning are part of the organisation's integrated management As part of the ATM security management system, a business continuity system is implemented	SeMS and its constituents (incident management) Documented crisis management and contingency plans approved by the NSA or the AA Documented plan for critical infrastructure protection (if applicable)	1. Documented exercises on crisis and contingencies, including results and lessons learnt				
					2. Documented list of roles and responsibilities for crisis and contingencies, including interfaces and points of contact with the NCASP and national crisis management. If applicable, interface with the EACCC (European Aviation Crisis Coordination Cell in the Network Manager) and critical infrastructure protection authorities				
					3. Documented list of both predefined and 'unknown' security scenarios for crisis and contingencies within the crisis management and contingency plans				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
			<p>for the full spectrum of threats identified in the threat assessment of the organisation to guarantee that the organisation is able to deliver the appropriate service level, even in a degraded mode during contingencies The organisation complies with applicable national and international legislation and requirements for critical infrastructure protection</p>		<p>4. Documented list of: dissemination and escalation procedures; measures for early threat detection, incident prevention and response mechanisms; security breach detection, incident identification, awareness and notification; incident reports, recovery actions, lessons learnt and implementation of corrective measures to improve the crisis management and contingency plans</p>				
10	Training	- ICAO Annex 17, chapter	ATM security culture is	SeMS and its constituents	1. ATM security training chapter within the SeMS				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
		3.1 - ICAO AVSEC Manual, 8 <sup>th</sup> Edition, Chapter 8 - EC 1035/2011, Annex I, Paragraph 5	embedded within the organisation The ATM Security training function is executed as part of the SeMS and integrated into the National Civil Aviation Security Training Programme (NCASTP)	(training programme) Documented training programme approved by the NSA or the AA and integrated into the National Civil Aviation Security Training Programme (NCASTP)	2. Documented ATM security training needs and requirements identified in the SeMS. Documented security culture, education, awareness, training and exercise plan; qualifications, training centres, training staff, security job profile definitions, accreditations, official recognition, training categories, security awareness for all staff etc. (to meet the security needs and requirements)  3. Documented established clear roles and responsibilities for ATM security training  4. ATM security training includes both self-protection and collaborative support aspects				
11	Safety/Security Interface	- ICAO AVSEC Manual, 8 <sup>th</sup> Edition, Chapter 9 - EC	Security management is integrated or at least coordinated	SeMS and its constituents (safety and security interface)	1. Documented Risk Management processes are part of the SeMS, consider all hazards approach/full				



#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y   On   N Going			
		1035/2011, Annex I, Paragraph 4 (Note: regulation 1035 does not include safety/security integration as a <u>requirement</u> . Literally, it says: 'The safety, quality and security management systems <u>may be</u> designed and operated as an integrated management system.')	and aligned with safety management (and ideally with other management systems e.g. Quality) in order to exploit synergies, avoid overlaps and make sure that security developments do not jeopardise safety and vice versa (In case of an integrated safety/security/quality management system, it should cover all aspects of a security management system)	definition) Documented process of safety/security (and ideally quality) integration, coordination and alignment, included in integrated corporate security/safety (and ideally quality) management systems of ANSP, AO and other applicable entities	<p>spectrum of threats (safety and security) and are managed at the highest corporate level</p> <p>2. Clear documented and established roles and responsibilities for corporate risk management</p> <p>3. Documented safety and security managers coordination meetings</p> <p>4. Documented joint complementary multidisciplinary internal audits and inspections for safety and security (and quality if applicable)</p>				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES	
						Y   On   N Going				
12	Security information exchange	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, Chapter 4</li> <li>- ICAO ATM Security Guidance</li> </ul>	<p>As part of the ATM security management system, security information exchange between national authorities, security and intelligence organisations and ATM security managers is implemented. It includes security warnings, threat and alert levels, incident identification and notification (i.e. security breaches), reporting and incident resolution follow-up.</p>	SeMS and its constituents (security information exchange) in the framework of the NCASP	<p>1. Documented arrangement for security information exchange e.g. with airports, AO, Military, AA, NSA, security and intelligence organisations</p>					
						<p>2. Documented exchange of security information e.g. security warnings, threat and alert levels, incident notification, threat assessments and incident reports</p>				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
13	Organisational , physical and technical security	<ul style="list-style-type: none"> <li>- ICAO AVSEC Manual, Chapter 5 and 8</li> <li>- ECAC Doc. 30, Chapter 13</li> </ul>	Security is fully embedded in the organisation's business plan and endorsed by management Roles and responsibilities are clearly defined The organisation, together with physical and technical means constitute a robust and resilient security system ensuring the protection of people, facilities and information, preventing unauthorised physical access, damage or interference	A documented process within the SeMS addressing organisational, physical and technical security	1. Security organisation chart approved by senior management and communicated to all staff through the awareness plan				
					2. Roles and responsibilities and job descriptions are clearly documented, endorsed and communicated to all staff. It includes: security manager, security experts, ICT security officer, risk assessors, security auditors/inspectors and security instructors				
					3. Documented security plan describing all security measures (physical, technical and procedural) to ensure the protection of people (staff and visitors) e.g. fencing, access control etc.				
					4. Documented description of the technical security system, features and				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA Y   On   N Going			CORRECTIVE ACTIONS & COMPLETION DATES
			with personnel, premises, assets or information of the organisation		performance in support of the physical security of people and facilities of the organisation e.g. cameras, intrusion detection, movement control, scanners etc.				
14	Information access control	- ICAO AVSEC Manual, Chapter 2	Access to classified and sensitive information relevant to aviation and ATM is restricted to those persons requiring such information in the performance of their duties Such information is protected from unauthorised access	SeMS and its constituents (security of information in line with national policies and provisions in the NCASP) A documented process addressing <u>Information Access Control</u> ; to control access to sensitive or classified information in order to protect information, in accordance with the 'Need	1. Documented part of the SeMS addressing the system for protection of information  2. Nomination by the senior corporate manager of a security officer responsible for the protection of information. This nomination and its job description is communicated to all staff. This security officer can be the same as the one described in bullet 4 Human Resources Security)  3. Documented list of means (human and material) allocated to the security officer to perform his/her duties				

#	REQUIREMENT	REGULATORY FRAMEWORK	EXPECTATIONS	MEANS OF COMPLIANCE	EVIDENCE	COMPLIANCE ASSESSMENT BY NSA			CORRECTIVE ACTIONS & COMPLETION DATES
						Y   On   N Going			
				to Know' principle (It can be soft or hard information and documentatio n)	4. Documented security education and awareness activities for staff regarding protection of information				
					5. Catalogue of classified material				
					6. Records of access to classified information				

**APPENDIX 3      Specific Questionnaire on Cyber Security**

QUESTIONS					
1      Security Governance					
	Area of Concern	Today	Future	Comment	Quick Wins/Action Plan
1.1	Does senior executive management provide strategic-level guidance that ensures compliance with security policies, standards and procedures?			Is a senior executive accountable for INFOSEC?	
1.2	Does senior executive management provide personnel a robust and effective security governance framework in which key business processes are integrated/covered?	yes		Well defined Roles and Responsibilities are needed to be effective and will reduce the likelihood of actual or perceived conflicts of interest	
1.3	Is a high level committee in place to control the security programme?			A high level committee typically consists of a senior executive (champion), critical business owners, CSO and CIO	
1.4	<b>INFOSEC documentation</b>				
1.4.1	Is a comprehensive and business-focused INFOSEC policy available, which is well communicated within the organisation?	partially	yes	The INFOSEC policy sets strategic direction and allows management to communicate its goals and expectations	
1.4.2	Security risk management plan	not yet	partially	The risk management plan supports the risk-based INFOSEC approach, determines the threats and vulnerabilities, list the selected controls to mitigate those risks, based on the organisation's risk appetite	

QUESTIONS					
1.4.3	Security incident management plan	not yet	yes	An incident management plan describes the actions to take in case of an INFOSEC incident which could compromise the organisation's business commitments. These actions should be flexible enough to cover most incidents, both already anticipated as well as completely unknown situations.	1/ Organisations should ensure that they have written incident response procedures which include a definition of personnel roles for handling incidents. The procedures should define the different phases of incident handling. 2/ Organisations should assign job titles and duties for handling computer and network incidents to specific individuals. 3/ Organisations should define management personnel that will support the incident handling process within each organisation, acting in key decision-making roles.
1.4.4	Business Continuity Management (BCM) plan	NA	partially	BCM defines the actions to be taken to survive emergency situations which potentially go well beyond INFOSEC and which could endanger the survival of the organisation	
1.4.5	Does the organisation use a data classification scheme?				
1.5	Is there an INFOSEC function?			The Chief Security Officer (CSO) is the ultimate responsible for day-to-day INFOSEC activities within the organisation	
1.6	Do large organisations have local INFOSEC coordinators which are competent to fulfil their duties and which have the mandate to suggest or even decide on actions?			Local INFOSEC experts should have the necessary tools and means to perform their work. They should have the appropriate authority level to swiftly respond to emergencies if needed.	
1.7	Is there an INFOSEC awareness programme?			The awareness programme provides INFOSEC information to staff clearly explains roles and responsibilities and is fully supported by senior executive management. INFOSEC training on how to run operations correctly is an important element of the awareness programme.	
1.8	<b>Cyber Security</b>				

QUESTIONS					
1.8.1	Does the organisation make use of the internal relationships across the organisation (e.g. crisis and incident management, business continuity management and internal audit)?			The organisation should have an organisation-wide action plan in case a cyber incident would occur. A well-defined communication and action plan will allow for faster responses to these incidents.	
1.8.2	Does the organisation gather cyber intelligence?			E.g. threat reports, cyberspace activity trends, incident reports (both from internal and external sources)	
1.8.3	Does the organisation have a cyber resilience programme?			A resilience programme typically consists of a cyber assessment and action plan based on the results of the assessment. This action plan can include both pro-active as well as reactive measures to respond to potential cyber threats.	
2 Risk and Incident Management					
	Area of Concern	Today	Future	Comment	Quick Wins/Action Plan
2.1	<b>Risk Management</b>				
2.1.1	Are risk assessments carried out for <u>all</u> business functions?			Risk assessments cover Business Impact Analysis (BIA), Threat & Vulnerability Assessment (T&V) and Control Selections (CS)	
2.1.2	Are risk assessments carried out for all <u>critical</u> business functions?			Risk assessments cover Business Impact Analysis (BIA), Threat & Vulnerability Assessment (T&V) and Control Selections (CS)	
2.1.3	<b>Business Impact Analysis (BIA)</b>				
2.1.3.1	Is the BIA carried out as part of the risk assessment process?			The BIA looks at the possible impact on the business functions when an INFOSEC incident would occur	



QUESTIONS					
2.1.3.2	Is the BIA carried out to select those processes which would be subject to a Threat & Vulnerability (T&V) and Control Selection (CS)?			The BIA looks at the possible impact on the business functions when an INFOSEC incident would occur	
2.1.4	Is the Threat & Vulnerability (T&V) carried out as part of the risk assessment process?			The T&V assessment looks at possible threats to the Confidentiality, Integrity and Availability of business process assets and possible vulnerabilities in the defence strategies of those assets	1/ Organisations should run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis. Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability scanning tool.2/ Organisations should ensure that vulnerability scanning is performed in authenticated mode (i.e. configuring the scanner with administrator credentials) at least quarterly, either with agents running locally on each end system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested to overcome limitations of unauthenticated vulnerability scanning.3/ Organisations should compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.4/ Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorised services. The tools should be further tuned to identify changes over time on systems for both authorised and unauthorised services. Organisations should use government-approved scanning configuration files for their scanning to ensure minimum standards are met.
2.1.5	Is the Control Selection (CS) carried out as part of the risk assessment process?			Based on a T&V specific controls are selected to increase the protection level of assets, resulting in an increased security level of the business processes themselves	
2.1.6	Is risk assessment an iterative process?			Risk assessments should be carried out with the introduction of new business processes or with an important change in an existing business process	

QUESTIONS					
2.1.7	Are the results of the risk assessments communicated to the business process owners?			A risk assessment report should at least contain the following elements: identification of the risks, the BIA of the risks, recommended actions (which can be risk acceptance , risk mitigation or transfer of risks)	The recommended and agreed actions must be officially signed off by the business owner
2.1.8	Are the results of the risk assessments signed off by the business process owners?			Acceptance of the risk assessment results by the business process owners is an important step of responsibility acknowledgement by the process owner	
2.2	<b>Incident Management</b>				
2.2.1	Is the Incident Management process well documented?				
2.2.2	Does the Incident Management process cover the 4 vital steps, which are Identification, Response, Recovery and Post-Incident reviews?			An RACI model serves the purpose of a clear Incident Management process by defining who is Responsible, Accountable, Consulted and Informed about possible recovery actions	
2.2.3	Are serious incidents escalated to executive management level?				
2.2.4	Is there an Emergency Response Team with clear responsibilities and an adequate level of authority?				
2.2.5	Does the Emergency Response Team have the capacity of doing forensic research and reporting?				
<b>3 Compliance Management</b>					
	<i>Area of Concern</i>	<i>Today</i>	<i>Future</i>	<i>Comment</i>	<i>Quick Wins/Action Plan</i>

QUESTIONS					
3.1	Has a method been established to identify and interpret the INFOSEC requirements of relevant laws and regulations?			All levels of the organisation should be consulted regarding existing laws and regulations which could have an impact on the organisation's business functions	
3.2	Is a review cycle in place to monitor compliance, which corrective actions, where needed?			The review cycle process should ensure compliance for all regulatory obligations or provide an action plan to implement those obligations	
3.3	Is personal data privacy and personal data protection part of the compliance review process?			Personally identifiable information should be treated in accordance to relevant legislation, such as the EU Directive on Data Protection	
<b>4 Technology Management</b>					
	<i>Area of Concern</i>	<i>Today</i>	<i>Future</i>	<i>Comment</i>	<i>Quick Wins/Action Plan</i>
4.1	<b>Asset Management</b>				
4.1.1	Do all assets meet the organisation's quality requirements (e.g. reliable hardware and software; asset accreditation)?			Most organisations have a list of accredited suppliers, approved software...	

QUESTIONS					
4.1.2	Is the asset inventory up to date?			Any change or update of assets should be reflected in the inventory. An adequate change management procedure will help achieve this.	<p>1/ Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to the enterprise network. Both active tools that scan through network address ranges, and passive tools that identify hosts based on analysing their traffic should be employed.</p> <p>2/ Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, and an asset owner responsible for each device. The inventory should include every system which has an IP address on the network, including, but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, Storage Area Networks, Voice-over-IP telephones, etc.</p> <p>3/ Ensure that network inventory monitoring tools are operational and continuously monitoring, keeping the asset inventory up-to-date on a real-time basis, looking for deviations from the expected inventory of assets on the network, and alerting security and/or operations personnel when deviations are discovered.</p>
4.1.3	Are software license requirements met?				<p>1/ Floating Software Licenses will help control the cost</p> <p>2/ Devise a list of authorised software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses</p>
4.1.4	Are the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) known for all critical assets?			The RTO and RPO will result in appropriate protection mechanisms for those critical assets (e.g. an Uninterruptible Power Supply (UPS) can protect a critical server from power outages; system mirroring will increase the availability of highly critical systems)	

QUESTIONS					
4.1.5	Is physical access to critical assets limited to authorised personnel?			A single layer of physical security, such as an identification pass for building access, is insufficient. The principle of Defence in Depth should also be applied here so additional credential checks should be carried out before giving access to critical assets.	
4.1.6	Are critical assets covered by a Service Level Agreement (SLA) with the supplier?			An appropriate SLA will raise awareness about the importance of assets with the supplier (proactive) and will reduce the time to repair in case of serious problems (reactive)	
4.1.7	Are the normal operating procedures known and explained in an Acceptable Use Policy (AUP), known by all personnel?			A clear understanding of the operating procedures and functions will increase the security awareness	
4.2	<b>Servers</b>				

QUESTIONS					
4.2.1	Are the Operating Systems of the critical servers hardened?			Hardening of a system is the process of reducing its "surface of vulnerability" to decrease the risk factor	<p>1/ System images must have documented security settings that are tested before deployment, approved by an agency change control board, and registered with a central image library for the agency or multiple agencies. These images should be validated and refreshed on a regular basis (such as every six months) to update their security configuration in light of recent vulnerabilities and attack vectors.</p> <p>2/ Standardised images should represent hardened versions of the underlying operating system and the applications installed on the system, such as those released by NIST, NSA, DISA, the Centre for Internet Security (CIS), and others. This hardening would typically include removal of unnecessary accounts, as well as the disabling or removal of unnecessary services. Such hardening also involves, among other measures, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and host-based firewalls.</p> <p>3/ Any deviations from the standard build or updates to the standard build should be documented and approved in a change management system.</p> <p>4/ The master images themselves must be stored on securely configured servers, with integrity checking tools and change management to ensure only authorised changes to the images are possible. Alternatively, these master images can be stored in off-line machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.</p>
4.3	Networks				

QUESTIONS					
4.3.1	Are network devices configured to function as required?			Does the configuration respect the security requirements?	<p>1/ Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed and approved by an agency change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.</p> <p>2/ At network interconnection points, such as Internet gateways, inter-agency connections, and internal network segments with different security controls, implement ingress and egress filtering to allow only those ports and protocols with a documented business need. All other ports and protocols besides those with an explicit need should be blocked with default-deny rules by firewalls, network-based IPSs, and/or routers.</p>
4.3.2	Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) installed on the network?			IDS and IPS facilitate the monitoring of the network on possible irregular network traffic, which might indicate a security breach	<p>1/ Network filtering technologies employed between networks with different security levels (firewalls, network-based IPS tools, and routers with ACLs) should be deployed with capabilities to filter IPv6 traffic. Even if IPv6 is not explicitly used on the network, many operating systems today ship with IPv6 support activated, and therefore filtering technologies need to take it into account.</p> <p>2/ Deploy IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These IDS sensors may detect attacks through the use of signatures, network behaviour analysis, or other mechanisms to analyse traffic.</p>
4.3.3	Are network devices configured to prevent unauthorised changes?				

QUESTIONS					
4.3.4	Are network devices configured to prevent unauthorised WIFI connections?				<p>1/ Organisations should ensure that each wireless device connected to the network matches an authorised configuration and security profile, with a documented owner of the connection and a defined business need. Organisations should deny access to those wireless devices that do not have such a configuration and profile.</p> <p>2/ Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorised wireless access points. Unauthorised (i.e. rogue) access points should be deactivated.</p> <p>3/ Organisations should ensure that all wireless access points are manageable using enterprise management tools. Access points designed for home use often lack such enterprise management capabilities and should therefore be avoided in enterprise environments.</p>
4.3.5	Is WIFI traffic encrypted?				
4.3.6	Is a VPN used for WIFI access?				
4.3.7	Are network devices well documented?			Incomplete network documentation will eventually lead to difficult to trace problems	
4.3.8	Are firewalls installed to protect critical systems?			Multiple DMZ zones can be created to cover increasing levels of protection	



QUESTIONS					
4.4	DMZ			<p>1/ Organisations should deny communications with (or limit data flow to) known malicious IP addresses (blacklists) or limit access to trusted sites (white lists). Periodically, test packets from bogon source IP addresses should be sent into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses (un-routable or otherwise unused IP addresses) are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.</p> <p>2/ Deploy IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These IDS sensors may detect attacks through the use of signatures, network behaviour analysis, or other mechanisms to analyse traffic.</p> <p>3/ On DMZ networks, monitoring systems (which may be built-in to the IDS sensors or deployed as a separate technology) should be configured to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border.</p> <p>4/ Define a network architecture that clearly separates internal systems from DMZ systems and extranet systems. DMZ systems are machines that need to communicate with the internal network as well as the Internet, while extranet systems are systems whose primary communication is with other systems at a business partner.</p>	
4.5	<b>Access Control</b>				
4.5.1	Is an appropriate Identity Management System in place?			<p>Proper Identity Management will among other things take care of sign-on procedures, authentication, authorisation, strong stringent authentication for critical systems</p>	

QUESTIONS					
4.5.2	Are security events logged and monitored?			Security logs are important but protecting these security logs against unauthorised change is equally important	<p>1/ Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis so that log files will not fill up between log rotation intervals.</p> <p>2/ System administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, identify anomalies more rapidly and prevent overwhelmed analysts with insignificant alerts.</p> <p>3/ All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely.</p> <p>4/ Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g. a file or directory) without the appropriate permissions.</p> <p>5/ Security personnel and/or system administrators should run bi-weekly reports that identify anomalies in logs. They should then actively review anomalies and document their findings.</p> <p>6/ Each agency network should include at least two synchronised time sources from which all servers and network equipment retrieve time information on a regular basis, so that timestamps in logs are consistent.</p>
4.5.2.1	Are server security events logged?				
4.5.2.2	Are workstation security events logged?				
4.5.2.3	Are network security events logged?				
4.5.2.4	Are radar security events logged?				
4.5.2.5	Are user security events logged?				

QUESTIONS					
4.5.3	Controlled use of admin privileges				<p>1/ Organisations should inventory all administrative passwords and validate that each person with administrative privileges on desktops, laptops, and servers is authorised by a senior executive and that his/her administrative password has at least 12 semi-random characters</p> <p>2/ Before deploying any new devices in a networked environment, organisations should change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.</p> <p>3/ Organisations should configure all administrative-level accounts to require regular password changes on a 30-, 60-, or 90-day interval.</p> <p>4/ Passwords for all systems should be stored in a hashed or encrypted format. Furthermore, files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges.</p> <p>5/ Organisations should ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.</p>

QUESTIONS					
4.5.4	Accounts monitoring & control				<p>1/ Systems should automatically create a report on a daily basis that includes a list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.</p> <p>2/ Organisations should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.</p> <p>3/ Organisations should monitor account usage to determine dormant accounts that have not been used for a given period, such as 30 days, notifying the user or user's manager of the dormancy. After a longer period, such as 60 days, the account should be disabled.</p> <p>4/ On a periodic basis, such as quarterly or at least annually, organisations should require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors.</p> <p>5/ When a dormant account is disabled, any files associated with that account should be encrypted and moved to a secure file server for analysis by security or management personnel.</p>
4.5.5	Penetration testing				<p>1/ Organisations should conduct regular penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e. the Internet or wireless frequencies around an organisation) as well from within its boundaries (i.e. on the internal network) to simulate both outsider and insider attacks.</p> <p>2/ Organisations should perform periodic red team exercises to test the readiness of organisations to identify and stop attacks or to respond quickly and effectively.</p>
4.6	<b>Change Management</b>				
4.6.1	Is the Change Management process well documented?				

QUESTIONS					
4.6.2	Is the Change Management procedures kept up-to-date?				
4.6.3	Are changes always tested in a test environment before being applied in the production environment?				
4.6.4	Is Patch Management part of the Change Management process?				
4.6.5	Are emergency fixes part of the Change Management process?				
4.6.6	Are emergency fixes reviewed after implementation?				

<b>ACTIONS AND TARGET DATES</b>			
<b>1 Security Governance</b>			
	<i>Area of Concern</i>	<i>Action</i>	<i>Target Date</i>
1.1	Does senior executive management provide strategic level guidance that ensures compliance with security policies, standards and procedures?		
1.2	Does senior executive management provide personnel a robust and effective security governance framework in which key business processes are integrated/covered?		
1.3	Is a high level committee in place which controls the security programme?		
1.4	<b>INFOSEC Documentation</b>		
1.4.1	Is a comprehensive and business-focused INFOSEC policy available, which is well communicated within the organisation?		
1.4.2	Security risk management plan		
1.4.3	Security incident management plan		
1.4.4	Business Continuity Management (BCM) plan		
1.5	Is there an INFOSEC function?		
1.6	Do large organisations have local INFOSEC coordinators which are competent to fulfill their duties and which have the mandate to suggest or even decide on actions?		
1.7	Is there an INFOSEC awareness programme?		
1.8	<b>Cyber Security</b>		
1.8.1	Does the organisation make use of the internal relationships across the organisation (e.g. crisis and incident management, business continuity management and internal audit)?		
1.8.2	Does the organisation gather cyber intelligence?		
1.8.3	Does the organisation have a cyber resilience programme?		
<b>2 Risk and Incident Management</b>			
	<i>Area of Concern</i>	<i>Action</i>	<i>Target Date</i>
2.1	<b>Risk Management</b>		

2.1.1	Are risk assessments carried out for <u>all</u> business functions?		
2.1.2	Are risk assessments carried out for all critical business functions?		
2.1.3	<b>Business Impact Analysis (BIA)</b>		
2.1.3.1	Is the BIA carried out as part of the risk assessment process?		
2.1.3.2	Is the BIA carried out to select those processes which would be subject to a Threat & Vulnerability (T&V) and Control Selection (CS)?		
2.1.4	Is the Threat & Vulnerability (T&V) carried out as part of the risk assessment process?		
2.1.5	Is the Control Selection (CS) carried out as part of the risk assessment process?		
2.1.6	Is risk assessment an iterative process?		
2.1.7	Are the results of the risk assessments communicated to the business process owners?		
2.1.8	Are the results of the risk assessments signed off by the business process owners?		
2.2	<b>Incident Management</b>		
2.2.1	Is the Incident Management process well documented?		
2.2.2	Does the Incident Management process cover the 4 vital steps, which are Identification, Response, Recovery and Post-Incident reviews?		
2.2.3	Are serious incidents escalated to executive management level?		
2.2.4	Is there an Emergency Response Team with clear responsibilities and an adequate level of authority?		
2.2.5	Does the Emergency Response Team have the capacity of doing forensic research and reporting?		
<b>3 Compliance Management</b>			
	<i>Area of Concern</i>	<i>Action</i>	<i>Target Date</i>
3.1	Has a method been established to identify and interpret the INFOSEC requirements of relevant laws and regulations?		
3.2	Is a review cycle in place to monitor compliance, which corrective actions where needed?		
3.3	Is personal data privacy and personal data protection part of the compliance review process?		
<b>4 Technology Management</b>			
	<i>Area of Concern</i>	<i>Action</i>	<i>Target Date</i>
4.1	<b>Asset Management</b>		

4.1.1	Do all assets meet the organisation's quality requirements (e.g. reliable hardware and software; asset accreditation)?		
4.1.2	Is the asset inventory up-to-date?		
4.1.3	Are software license requirements met?		
4.1.4	Are the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) known for all critical assets?		
4.1.5	Is physical access to critical assets limited to authorised personnel?		
4.1.6	Are critical assets covered by a Service Level Agreement (SLA) with the supplier?		
4.1.7	Are the normal operating procedures known and explained in an Acceptable Use Policy (AUP), known by all personnel?		
4.2	<b>Servers</b>		
4.2.1	Are the Operating Systems of the critical servers hardened?		
4.3	<b>Networks</b>		
4.3.1	Are network devices configured to function as required?		
4.3.2	Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) installed on the network?		
4.3.3	Are network devices configured to prevent unauthorised changes?		
4.3.4	Are network devices configured to prevent unauthorised WIFI connections?		
4.3.5	Is WIFI traffic encrypted?		
4.3.6	Is a VPN used for WIFI access?		
4.3.7	Are network devices well-documented?		
4.3.8	Are firewalls installed to protect critical systems?		
4.4	<b>Access Control</b>		
4.4.1	Is an appropriate Identity Management System in place?		
4.4.2	Are security events logged and monitored?		
4.4.2.1	Are server security events logged?		
4.4.2.2	Are workstation security events logged?		
4.4.2.3	Are network security events logged?		
4.4.2.4	Are radar security events logged?		
4.4.2.5	Are user security events logged?		
4.5	<b>Change Management</b>		
4.5.1	Is the Change Management process well-documented?		



4.5.2	Is the Change Management procedures kept up-to-date?		
4.5.3	Are changes always tested in a test environment before being applied in the production environment?		
4.5.4	Is Patch Management part of the Change Management process?		
4.5.5	Are emergency fixes part of the Change Management process?		
4.5.6	Are emergency fixes reviewed after implementation?		

yes  
partially  
not yet  
NA

## **Appendix 4: Guidance for ATM Security Oversight Planning Security Oversight Programme**

### **1. INTRODUCTION**

ATM security oversight is a component of the National Civil Aviation Security Quality Control programme (NCASQCP or NQCP). Generic guidance on quality control is provided in ICAO AVSEC Manual, Chapter 7. According to the ICAO manual, one of the main objectives of the NQCP is to ensure the effectiveness of State regulations and the NCASP.

The NQCP should be developed and maintained in cooperation with all entities involved in implementing aviation security measures and the programme should be explained to any entity that could be subject to quality control activities such as airports, aircraft operators and air navigation service providers.

Due to the disparity of ANSP and ATM players in different States, ATM security quality control measures must be tailored to fit each State's particular aviation environment and needs.

### **2. PRINCIPLES**

#### **2.1 Objective**

The ATM security oversight programme should provide for required verifications that all applicable regulatory measures are efficiently implemented by the ANSPs and other entities subject to the NQCP, under the responsibility of the State authority; AA and NSA.

#### **2.2 Policy**

ATM security oversight must follow the principles and policies laid down in the NCASP. Chapter 3 provides elements for policy and planning of ATM security.

The development of a national annual ATM security oversight programme should be based on priorities determined by the AA and the NSA and take into account resources and time constraints.

#### **2.3 Authority**

According to ECAC Doc. 30; 'the State should designate the relevant authority within its administration to be responsible for the oversight and coordination of ATM security'. The Single European Sky (SES) regulatory framework requires States to designate an NSA (National Supervisory Authority) responsible for the oversight of common requirements including some security requirements (laid down in Commission Implementing Regulation (EC) N° 1035/2011, Annex I, Paragraph 4; see Chapter 2 of this manual). It should be noted that these requirements do not cover the full spectrum of ATM security requirements (see security questionnaires in Appendixes 1 and 2). Therefore, if designated as the State authority for ATM security oversight, the NSA should not restrict his/her activities to the SES regulatory framework but cover the full spectrum of ATM security requirements (including those stemming from national specific legislation).

To this end, the single authority responsible for the national ATM security oversight programme must establish clear links with other authorities responsible for aviation and ATM security e.g. CAA, AA and NGA.

Table 4 is provided hereafter as example.

Title	Name	Department Organisation	Function	Contact Details
Mr		CAA/NSA/AA/...	State Authority for ATM Security Oversight	Official postal address Tel/fax/GSM/email/H14 contact means (if required)
Mrs		CAA/NSA/AA/...	Deputy State Authority for ATM Security Oversight	
Dr		CAA/NSA/AA/...	Assistant State Authority for ATM Security Oversight	
...	...	...	...	...

**Table 3: ATM Security Oversight Authority**

Together with the official designation of the single authority responsible for the national ATM security oversight programme, the entities within the aviation system **subject to security oversight** by this authority should be established and communicated. Typically, it will be the ANSP operating in the State; however, national legislation might extend the competences of the authority to other entities e.g. AO and Airports (air side).

## 2.4 Legal Basis

The State authority for ATM security oversight must be properly empowered by national legislation to perform his/her duties. The same applies to the security inspectors and auditors.

## 2.5 ATM Security Inspectors and Auditors

Inspectors and auditors are the same person; only the function changes (see Annex B, Definitions).

According to the ICAO AVSEC Manual, Chapter 7, there are several ways to the monitor civil aviation security systems:

Monitoring Activity	Content	Characteristics
Security audit	In-depth (as exhaustive as possible) examination of <b>all</b> aspects of the NCASP requirements	<input type="checkbox"/> Timing: from a number of days to one month <input type="checkbox"/> Multi-site/location <input type="checkbox"/> Should always be announced in advance <input type="checkbox"/> Should not include overt or cover security tests

Monitoring Activity	Content	Characteristics
Security inspection	Examination of implementation of relevant provisions in the NCASP	<input type="checkbox"/> Narrower scope than an audit <input type="checkbox"/> Focuses on a specific activity <input type="checkbox"/> May be announced in advance <input type="checkbox"/> May include overt or cover security tests
Security test	Simulation of an attempt to commit an unlawful act to test a security measure	<input type="checkbox"/> May be overt or cover security tests <input type="checkbox"/> Only demonstrate if a security measure or control proved effective at a specific place and time <input type="checkbox"/> Focus on access control to restricted areas, protection of assets etc,
Security survey	Evaluation of security needs	<input type="checkbox"/> Is intended to: <ul style="list-style-type: none"> <li>○ Highlight vulnerabilities that could be exploited to carry out an act of unlawful interference</li> <li>○ Recommend corrective actions</li> </ul> <input type="checkbox"/> Should be carried out whenever a threat necessitates an increased level of security <input type="checkbox"/> The scope ranges from targeted assessment focused on a specific operation to an overall evaluation of security measures <input type="checkbox"/> Timing: from a few hours to several weeks <input type="checkbox"/> Should include overt or covert security tests

**Table 4: Types of Monitoring Activities**

Inspectors and auditors are the core element of the NQCP. They must be provided with:

- Legal framework: describe their responsibilities and empower them to exercise those responsibilities and perform their duties;
- Training and qualifications: provide them with the required skills to carry out audits and inspections;
- Certification: specific diplomas accrediting required knowledge, skills and performance are met by the individual. It should include renewal and upgrading criteria;
- Confidentiality clause: states the conditions and circumstances under which information gathered during their oversight activities can or cannot be disclosed. It will include the level of classification of the security reports or parts of them, and the associated required security clearances to handle such information;

- Independence: it is twofold; on the one hand it should be guaranteed that inspectors and auditors perform their duties under no undue pressure. On the other hand, they should carry out their functions in an impartial, fair and reliable manner.

The State authority for ATM security oversight must keep an up-to-date list of auditors. The table below is provided as an example.

It should be noted that many aspects of security oversight are common to all aviation security areas, disregarding if they refer to an airport, an ACC or an aircraft operator centre. For example, oversight of physical security, personnel security, organisational security and cyber security do not require different skills for auditors of ANSP, airports or AO. A period of familiarisation with one or other operational environments should suffice. This consideration is extremely important because it provides a possibility to build on the experience of existing practices for aviation security oversight and, much more relevant, to **re-use aviation security inspectors for ATM security oversight**. In other words, aviation security inspectors/auditors are by default ATM security inspectors/auditors.

It is important to insist and clarify that there is no need for a separate setup of 'ATM security auditors'. In the single title "**aviation security auditor (or inspector)**" the ATM competencies are included in the same manner that ATM security belongs to aviation security and ATM security oversight is part of the NQCP. The only requirement is to provide the inspectors with the appropriate training to be able to perform their duties in the ATM environment.

These training needs should be included in the NASTP. In the same way, there is no need to create separate training requirements and courses. Existing security auditor courses should cater for ATM security training needs. Specific training modules should be added or adapted if needed to cover all aspects of ATM security, not included in the current aviation security training e.g. ATM security collaborative support, and make inspectors familiar with the ATM security environment.

Furthermore, in the specific case of cyber security it is most likely that cyber security experts and auditors could be inter-changeable not only within departments but also among departments themselves, which also constitutes an efficiency and cost saving factor. The rationale for this is that cyber security is by nature a transversal discipline which becomes more and more relevant, complex and important, not only for air transport but for the whole societal activity. This concept of inter-changeability of inspectors across departments is worth considering and implementing to optimise national resources in security oversight.

Security inspectors can also be obtained from:

- a third party e.g. industry bodies;
- relevant entities participating in the NQCP e.g. AO, ANSP, Airport Operators, government bodies. In this case, inspectors from a specific industry body should not perform oversight activities on an industry body of the same kind (e.g. an inspector coming from air navigation service provision should not inspect an ANSP);
- neighbouring countries e.g. in the context of FABs, if agreement for mutual recognition exists.

All security inspectors participating in ATM security oversight must be officially empowered and designated by the relevant authority (AA or NSA). These authorities must keep an up-to-date list of inspectors/auditors empowered, designated and qualified to carry out security aviation security oversight activities (audits, inspections, surveys and tests) within the State.

Auditor Code	Name	Department/Organisation	Role/Area
		NSA	Audit team leader(s)
		CAA Cyber security department	Security auditor(s) (cyber)
		AA/National Security Committee	Aviation security auditor(s)
		NSA	Aviation security auditor(s) (ATM)
		ANSP	Aviation security auditor(s) (SeMS)

**Table 5: List of Auditors/Inspectors for ATM Security Oversight**

**2.6 Harmonisation**

National ATM security oversight should make use of national and international best practices and standards. This will contribute to lifting the reputation of the State regarding ATM security management and reaching harmonisation across States.

**3. Methodology**

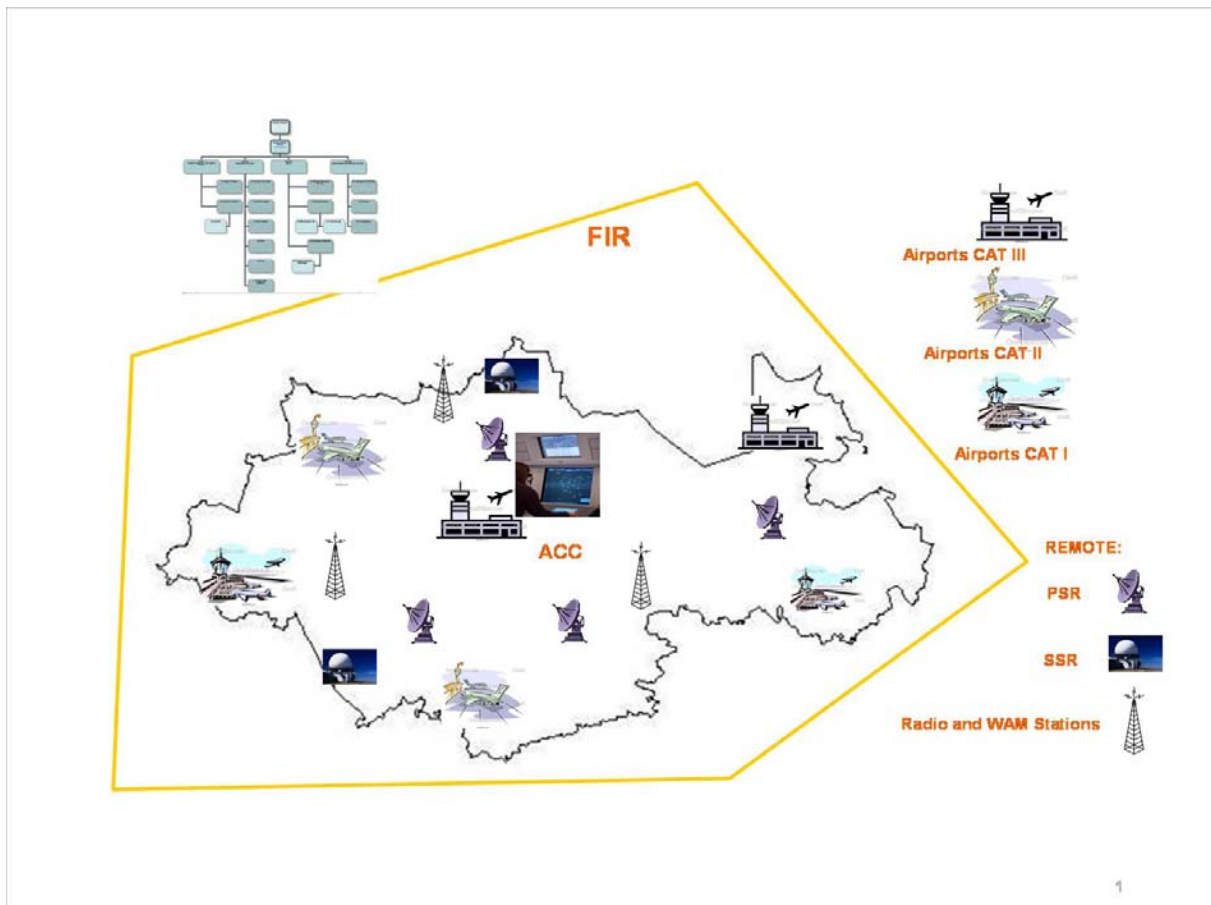
The AA/NSA should promote fluent communication and transparent dialogue with the entities to be audited/inspected. The following is a guide to establish work and a communication plan. Some milestones may be altered depending on the maturity of the audit programme e.g. if it is the first inspection ever or on the contrary, some or many inspections had already taken place.

It is the privilege of the AA/NSA to carry out unannounced inspections, nevertheless it is recommended not to do it at the initiation of the oversight programme, before getting familiar with the process and issues associated to security inspections. The oversight authorities should strive to minimise impact of unannounced inspections on normal operations.

ATM security oversight activities should be carried out in a standardised systematic way in order to achieve consistency in the consolidation and comparison of findings and recommendations.

The national authority responsible for ATM security oversight (AA/NSA) and the oversight teams should first get familiar with the entities subject to the oversight programme (see paragraph 2.3 in this appendix). This knowledge should include as a minimum:

- Mission of the entity
- Organisation chart
- Points of contact
- Geographical deployment (see example in figure 15 below)
- Asset inventory
- Initial oversight or ongoing oversight activity
- Previous audit reports/ongoing compliance issues



**Figure 15: Organisation and Deployment of a Fictitious ANSP**

Secondly, for **each entity** subject to security oversight a generic plan should be developed. The following phases should be considered in the work plan:

- Initiation
- Preparation
- Execution

### 3.1 Initiation

- The entity is informed in written by the national authority (for this example the NSA) that will be subject of security oversight, in line with national legislation and procedures. The entity is invited to acknowledge and provide any comment or concern;
- The NSA calls for a coordination meeting with the entity;
  - Explain the launching of the oversight programme (initial oversight or ongoing) starting next year;
  - Its background and legal basis e.g. security requirements;
  - Expectations from the NSA side;
  - Invites for feedback;

- o The entity informs about the current situation, problems encountered and corrective measures implemented;
- The NSA proposes an initial schedule for planned oversight activities for the following year (audits, inspections, tests and surveys)<sup>17</sup>;
- The entity provides remarks to the plan;
- The ATM security oversight **programme** is approved.

This programme consists of a **schedule of planned oversight activities** which are aimed at assessing the security maturity level of the entity and its compliance with the regulatory framework and associated security requirements.

The programme establishes a schedule of events that will be carried out during a twelve-month period. When required, there can be deviations from planned activities. Deviations should be coordinated between the authority (NSA) and the inspected entity and revisions and amendments issued.

The ATM security oversight schedule could be laid down in tables, charts, graphics or any other supporting tool to help the NSA visualise the milestones and oversight activities. The schedule should be flexible enough to accommodate non-scheduled activities. An easy example is provided in the table below.

Entity 1	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
HQ		X										
ACC			X									
APP/TWR					X							
Remote Site 1							X					
Remote Site 2									X			

**Table 6: Schedule for Security Oversight of an Entity**

Oversight activities can respond to 4 main reasons:

- Initial oversight e.g. for certification/designation of the entity;
- Scheduled oversight activities as per the approved ATM security oversight programme;
- Non-scheduled security oversight activities (inspections, surveys and tests) as required by the NSA to assess the impact of new or evolving threats or as a consequence of threat assessments;
- Follow-up audits/inspections to verify the implementation and effectiveness of corrective actions,

**The ATM security oversight programme must be an integral part of the overall National AVSEC programme and must be included in the NQCP.**

<sup>17</sup> The NSA retains its privilege to conduct non-announced in advance inspections, surveys and tests



### 3.2 Preparation

For **each oversight activity** within the programme, a number of preparatory activities take place. The most relevant are:

1. Preparatory phase. As a general rule, it should last a minimum of 10 weeks prior to the audit/inspection. It includes preparation and review of documents. The NSA must appoint an audit team **leader** who should compose his/her audit **team** in accordance with the nature of the oversight activity and the entity subject.

A standard audit team is composed of:

- A team leader;
- Security inspectors: the required number of inspectors and their qualifications should cover all sites and areas to be inspected e.g. cyber security, communications security, SeMS, threat assessments, physical/personnel/technical/organisational security;
- (An) assistant(s)

Audit team actions (desktop audit):

- Identify the objective and scope of the oversight activity;
- Contact the target entity; provide the list of security **Requirements** and **Expectations** (see Appendix 2);
- Request proposed **Means of compliance** and **Evidence** against high level requirement and expectations;
- Obtain copy of relevant documents;
- Review documentation; compare against requirements;
- Check where compliance against criteria is not documented; provide feedback to the entity for possible corrections;
- Develop schedule for on-site audit;
- Define audit lots for each audit team member;
- Develop **detailed questionnaires**/checklists; detailed questionnaires can be totally or partly shared with the entity,

### 3.3. Execution

The following are basic milestones in the execution of an oversight programme:

2. Visiting Phase
  - Conduct of on-site audit(s)/inspection(s). It should be based on the detailed questionnaires/checklist. However, the audit team is legitimate to address any other issue as required;
  - It includes interviews with all relevant security players at the entity,

3. Reporting phase. As a general rule, it should last a maximum of 12 weeks following the audit/inspection;
- **Assessment** by the audit team. A final report must be issued in a standard format addressing all findings of the audit/inspection including the assessment of security compliance;
  - The report must be formally submitted to the entity;
  - It must clearly identify any corrective action needed, including time of completion;
  - A corrective action plan must be proposed by the entity and approved by the audit team leader or the NSA. The action plan must identify the corrective actions with immediate priority, which requires action without delay. Proposals should address the “root cause” of the revealed problem.

A deficiency exists when the oversight activity reveals non-compliance with national regulations, NCASP provisions or international standards.

The level of compliance should be established in accordance with national requirements. Classifying the levels of compliance will help the audited entity prioritise corrective actions. The following compliance classification is provided by ICAO (AVSEC Manual):

- a) Category 1: meets the requirements;
- b) Category 2: does not meet the requirements and has minor deficiencies that need improvement;
- c) Category 3: does not meet the requirements and has serious deficiencies that need improvement;
- d) NA (not applicable): measure or procedure does not exist at the given airport or is not available;
- e) NC (not confirmed): when a measure has been either not verified or not observed due to a lack of time or other circumstances.

Corrective actions should deal with the root cause of the problem and when implemented should be fully effective in eliminating the identified non-compliance. In the case that effective corrective actions are not being taken by the entity or no indication is given as to when it will be fully implemented, the NSA may consider an enforcement action.

The various enforcement measures should be enacted through national legislation. They could include:

- Administrative actions:
  - Verbal advice for minor deficiencies, with record-keeping as official evidence;
  - Formal letter to the entity requiring a corrective action and expected outcome in case of a serious deficiency;
  - Enforcement notice when serious deficiencies remain or in case of major deficiencies;
  - Revocation of certificate (EC 550/2004, Art. 7.7);
  - Monetary penalties;
- Judicial actions (if CAA is so empowered by the State legislation),

4. Follow-Up Phase. As a general rule, it should last a maximum of 16 weeks following the reporting phase.
  - The audit team must monitor, in coordination with the entity, the implementation of the corrective action plan;
  - Verify and close-out of corrective actions, when duly implemented;
  - Follow-up audits can be organised to verify implementation of corrective actions,

A follow-up audit is a formal activity conducted to verify implementation of corrective actions. This should be done after receiving details of the corrective actions proposed together with associated timescales.

5. Closure Phase, to take place at the end of the follow-up phase. It will mean that all corrective actions have been duly completed. All documentation relating to the audit/inspection should be filed and a letter sent to the entity informing of the closure of the activity.

The NSA must produce a report and keep a record of every oversight activity (audit, inspection, survey, test) in written form. Reports should include:

- date and place of the inspection;
- name of the entity;
- composition of the audit team;
- list of persons met or interviewed;
- the subject matter;
- security aspects observed;
- finding, results and level of compliance,

The reports must be classified and disseminated in accordance with national rules for the protection of classified or sensitive information.

#### **4. EASA STANDARDISATION INSPECTIONS & OTHER ACTIVITIES**

EASA carries out standardisation inspections in EASA Member States in accordance with Commission Regulation (EC) N° 736/2006, on working methods of the European Aviation Safety Agency for conducting standardisation inspections.

Every standardisation team is composed of an EASA team leader and team members seconded by NAA's (**National Aviation Authority**)<sup>18</sup>. The on-site phase of a standardisation inspection usually lasts one week. The teams also visit undertakings approved by that Member State's NAA to sample how the NAA performs its oversight obligations.

A final report is established after a standardisation inspection. It contains any findings against the NAA inspected and is sent to the NAA inspected, to the Member State's government and to the European Commission.

For non-compliance findings, the NAA must establish and implement remedial action plans within agreed timelines. The Agency in turn verifies and validates the satisfactory progressive implementation of action plans.

---

<sup>18</sup> NAA is a synonym of CAA

In addition to inspections, the EASA Standardisation Department also

- organises standardisation meetings with all NAA's;
- manages a web-based communication forum exchanging information with NAA's;
- conducts inspections in the framework of bilateral agreements and working arrangements;
- conducts accreditation inspections where NAA's perform certain oversight tasks on behalf of the Agency;
- participates in ICAO Universal Safety Oversight Audit Programme (USOAP) audits;
- organises ad-hoc and follow-up inspections where required;
- provides technical experts to European Commission missions; and
- establishes the Agency's annual report on standardisation activities.

## ANNEX E – ATM Security Related Material Basic Documentation

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
<b>ICAO</b>			
1	Doc. 7300	Convention on International Civil Aviation	National ICAO PoC
2	Annex 17 to the Convention on International Civil Aviation	Security – Safeguarding International Civil Aviation Against Acts of Unlawful interference	National ICAO PoC
3	Doc. 8973 (Restricted)	ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference	National ICAO PoC
4	Cir. 330 AN/189	Civil Military Cooperation in Air Traffic Management	National ICAO PoC
5	Doc. 9985 (Restricted)	Air Traffic Management Security Manual	National ICAO PoC
<b>ECAC</b>			
1	Doc. 30 (Restricted)	ECAC policy statement in the field of aviation facilitation	National ECAC PoC
<b>EC</b>			
1	Regulation (EC) N° 549/2004 of the European Parliament and of the Council	Laying down the framework for the creation of the single European sky	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
2	Regulation (EC) N° 550/2004 of the European Parliament and of the Council	Provision of air navigation services in the single European sky	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
3	Regulation (EC) N° 1070/2009 of the European Parliament and of the Council	Amending Regulations (EC) N° 549/2004, (EC) N° 550/2004, (EC) N° 551/2004 and (EC) N° 52/2004 in order to improve the performance and sustainability of the European aviation system	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
4	Commission Regulation (EC) N° 2096/2005	Laying down common requirements for the provision of air navigation services	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
5	Commission Regulation (EC) N° 1032/2006	Requirements for automatic systems for the exchange of flight data for the purpose of notification, coordination and transfer of flights between air traffic control units	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
6	Commission Regulation (EC) N° 482/2008	Software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) N° 2096/2005	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
7	Regulation (EC) N° 300/2008 of the European Parliament and the Council	Common rules in the field of civil aviation security and repealing Regulation (EC) N° 2320/2002	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
8	Commission Regulation (EC) N° 272/2009	Supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) N° 300/2008 of the European Parliament and of the Council	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
9	Commission Regulation (EU) N° 18/2010	Amending Regulation (EC) N° 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security are concerned	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
10	Commission Regulation (EU) N° 73/2010	Laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
11	Commission Regulation (EU) N° 185/2010	Laying down detailed measures for the implementation of the common basic standards on aviation security	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
12	Commission Regulation (EU) N° 691/2010	Laying down a performance scheme for air navigation services and network functions and amending Regulation (EC) N° 2096/2005 laying down common requirements for the provision of air navigation services	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
13	Commission Regulation (EU) N° 77/2011	Laying down detailed rules for the implementation of air traffic management	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
		(ATM) network functions and amending Regulation (EU) N° 691/2010	
14	Commission Implementing Regulation (EU) N° 1035/2011	Laying down common requirements for the provision of air navigation services and amending Regulations (EC) N° 482/2008 and (EU) N° 691/2010	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
15	Commission Regulation (EU) N° 1141/2011	Amending Regulation (EC) N° 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
16	Commission Implementing Regulation (EU) N° 1147/2011	Amending Regulation (EU) N° 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
17	Commission Implementing Regulation (EC) N° 1087/2011	Amending Regulation (EU) N° 185/2010 laying down detailed measures for the implementation of the common basic standards on aviation security in respect of explosive detection systems	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
18	Commission Implementing Regulation (EU) N° 859/2011	Amending Regulation (EU) N° 185/2010 laying down detailed measures for the implementation of the common basic standards on aviation security in respect of air cargo and mail	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>
19	Council Directive 2008/114/EC	Identification and designation of European critical infrastructures and assessment of the need to improve their protection	<a href="http://eur-lex.europa.eu/en/index.htm">http://eur-lex.europa.eu/en/index.htm</a>

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
	Cybersecurity Strategy of the European Union:	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions from High Representative of the European Union for Foreign Affairs and Security Policy on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace The objective of the Strategy is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and other EU core values	<a href="http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf">http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf</a>
	Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union	This proposal is the main action of the Strategy above. The aim of the proposed Directive is to ensure a high common level of network and information security (NIS)	<a href="http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf">http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf</a>
<b>EUROCONTROL</b>			
1	Security Management Handbook		<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home</a> (restricted access)
2	ATM Security Risk Assessment Methodology		<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home</a> (restricted access)
3	Critical Asset Identification for ATM		<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home</a> (restricted access)
4	ICT Security Guidance material		<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home</a> (restricted access)
5	ATM Threat Model		<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/eatmpsecurity/home</a>



#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
			(restricted access)
6	Guidelines in developing an ANSP's Certification Process		I:\Single Sky\3-REGULATORY SUPPORT\CAA_NSA Unit\NSA Documentation - Training\Documentation (restricted access)
7	Guidelines for NSAs for the Development of the ANSP Designation Process		I:\Single Sky\3-REGULATORY SUPPORT\CAA_NSA Unit\NSA Documentation - Training\Documentation (restricted access)
8	Guidelines for ANSPs Oversight Process		I:\Single Sky\3-REGULATORY SUPPORT\CAA_NSA Unit\NSA Documentation - Training\Documentation (restricted access)
9	Guidelines for the development of a Handbook for National Supervisory Authorities		I:\Single Sky\3-REGULATORY SUPPORT\CAA_NSA Unit\NSA Documentation - Training\Documentation (restricted access)
<b>NATO/EUROCONTROL ATM Security Coordinating Group (NEASCOG)</b>			
1	AC/92(NEASCOG)D(2006)0001	ATM Security Strategy	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
2	AC/92(NEASCOG)D(2011)0001 EUROCONTROL(NEASCOG)D(2011)0001	Unmanned Aerial Systems (UAS) Security	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
3	AC/92(NEASCOG)D(2011)0002 EUROCONTROL(NEASCOG)D(2011)0002	Airspace Security Incidents	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
4	AC/92(NEASCOG)N(2011)0008 EUROCONTROL(NEASCOG)N(2011)0008	ICT Self-Assessment Security Questionnaire (draft)	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
5	AC/92(NEASCOG)D(2009)0001 EUROCONTROL(NEASCOG)D(2009)0001	Airspace Security Threat and Risk Assessment	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
6	AC/92(NEASCOG)D(2009)0003 EUROCONTROL(NEASCOG)D(2009)0003	Airspace Security Management High Level Concept	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a>

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
	09)0003		(restricted access)
7	AC/92(NEASCOG)D(2009)0004 EUROCONTROL(NEASCOG)D(2009)0004	NEASCOG Airspace Security Action Plan	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
8	AC/92(NEASCOG)D(2009)0005-REV1 EUROCONTROL(NEASCOG)D(2009)0005-REV1	Aviation Security Components	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
9	AC/92(NEASCOG)D(2010)0003 EUROCONTROL(NEASCOG)D(2010)0003	Airspace Security GA Issues	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
10	AC/92(NEASCOG)D(2010)0002 EUROCONTROL(NEASCOG)D(2010)0002	Airspace Security Technology Support	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
11	EUROCONTROL	ATM Security SWOT Analysis	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
12	AC/92(NEASCOG)WP(2009)0005 EUROCONTROL(NEASCOG)WP(2009)0005	Guidelines for Co-ordination Procedures to Harmonise at International Level the Handling of Suspected Renegade Situations	<a href="https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home">https://extranet.eurocontrol.int/http://beid.eurocontrol.be:8980/Members/irc/eurocontrol/neascog/home</a> (restricted access)
13	Guidelines for ATM Coordination in Crisis Situation	Guidelines for Co-ordination Procedures between NATO and EUROCONTROL and other entities, e.g. ICAO, in case of crisis leading to air operations with an impact on European airspace.	NATO PoC
<b>STANDARDS - International Organization for Standardization (ISO)</b>			
1	ISO 28000:2005	Security Management Standard	<a href="http://www.iso.org">www.iso.org</a>
2	ISO 27000:2009	Information security management systems	<a href="http://www.iso.org">www.iso.org</a>

#	DOCUMENT IDENTIFICATION	SUBJECT/CONTENT	AVAILABILITY
3	ISO 27006:2011	Requirements for bodies providing audit and certification of information security management systems	<a href="http://www.iso.org">www.iso.org</a>
4	ISO 18028:2005	IT network security	<a href="http://www.iso.org">www.iso.org</a>