APPENDIX / APÉNDICE

MANUAL ON THREAT ASSESSMENT AND RISK MANAGEMENT METHODOLOGY (Reference Guide for States)

PARTICIPATING STATES

CHILE
COLOMBIA
JAMAICA
DOMINICAN REPUBLIC

FOREWORD

The present work follows the agreement adopted by the Aviation Security and Facilitation Regional Group NAM/CAR/SAM OACI/CLAC (AVSEC/FAL/RG), during the first meeting held in Asuncion, Paraguay, between May 25 and 27, 2011. A Work Plan was agreed upon that considered among other topics the establishment of a regional threat level system through the preparation of a Threat Assessment and Risk Management Methodology manual. There were two objectives set forth:

1. - Establish a consistent methodology as a reference guide to assess threats and risk management at airports.

2. - Guide States through the application of preventive measures, based on an analytical and predictive method.

To carry out the work, a group of experts was established, with the representative of Chile serving as the coordinator and the representatives of Colombia, Dominican Republic and Jamaica as contributors.

1. - Reference material used

- Annex 17, Amendment 12
- Security Manual, Document 8973 Volume V
- Case Study 19 presented by the Bolivarian Republic of Venezuela
- Procedures of the Aviation Authority of the Republic of Colombia
- Procedures of the Aviation Authority of the Republic of Chile.

MANUAL ON THREAT ASSESSMENT AND RISK MANAGEMENT METHODOLOGY (Reference Guide for States)

CHAPTER I

Definitions

Threat
It is the quantification of the possibility/probability of an attack against a specific target

Threat Assessment
The estimation of the probability for an attack to be enacted against a target during a specific time frame.

Risk Assessment
The estimation of the probability that such attack is successful.

Vulnerability Assessment
The analysis of the target characteristics to establish the weaknesses that could be exploited in different attacks. The analysis shall determine the probability of those attacks being successful.

Security Study.
Assessment of the needs related to security, as well as identifying weaknesses that could be taken advantage of to commit an illicit act of interference, and the recommendation of corrective measures.

Intelligence
The result of processing all the data received and related to a specific target, through the search, processing, and distribution of useful information for decision making.

Risk
The probability of an attack against a target being successful.

Vulnerability
The characteristics of any target that could be exploited for an attack, or how easy it would be to attack the target.

CHAPTER II

Threats Assessment

Annex 17 “Security, Protection of International Civil Aviation against illicit acts of interference, states the following in Regulation 3.1.3.:
“Each contracting State shall assess constantly the threat level for civil aviation in their territory. Also, it shall establish policies and procedures to adjust the relevant aspects of their national security program for civil aviation based on a risk assessment evaluation for aviation by pertinent national authorities.”

Considering that one of the tasks for security aviation experts is to design an efficient and effective security system that responds to threats against civil aviation, a precise assessment of the threat(s) should be the first step in the process. The latter contributes directly to the risk assessment of airport security.

To contribute, together with the States of the Region, a manual on threat assessment and risk management methodology has been developed. This manual will allow an analytical approach that validates the information on an ongoing basis and, based on these data deploy human and technical resources.

States can delegate the responsibility of assessing threat types and levels against civil aviation to specialized organizations, such as intelligence service from a law enforcement, military or policy agency, according to what the States decide.

Assessment Methodology

When assessing threats, it is suggested that a systematic and quantifiable approach is used to assess one or more actual threats against an airport, aircraft operator or country. Therefore, three security principals must be considered in this methodology:

- Identifying the threat
- Applying an analysis and dissemination process
- Maintaining a follow-up and progress system

In order to assess threats against civil aviation, forecast processes should be used in the application of an intelligent risk management system for airport security.

Planning and Direction

Since a threat is the reckoning of a possibility or probability of an attack against a specific target taking place, in this phase the targets and requirement for Intelligent must be identified with precision, regarding threats against civil aviation at the national level. Some of these could be:

- Presence of terrorist groups
- Organized crime
- Anti-system groups
- Social conflicts

- Radical ethnic groups
- Religious sects
- Radical environmental groups
- Labor conflicts in airports

Considering there are several real data sources that have not been evaluated in the intelligence and airport security sectors, as well as other statistics available, the relevant authority appointed to assess threats must include in its policies, the search priorities to identify, eliminate or confirm the existence of an illicit association or organization representing a threat to civil aviation.

At the Planning and Direction stage, threats and their repercussions must be defined in air operations and in relation to travelers' safety. Such task must the translated into actual requirements by those responsible for making political decisions, such as the National Committee on Aviation Security, the Airport Authority or Civil Aviation.

Collecting Information

In this stage the raw data will be acquired and collected, in other words, the intelligence needed for aviation security. There are several open sources that provide useful information, such as responsible media, certain websites, NGOs, government entities reporting background information on crime rates in cities, migration flow data, indicators on weapons and drug trafficking in the region and the country. However, it is also important to have closed sources, such as technical, law enforcement agencies and other public entities; in addition, we can include international organizations and input from other States. In any case, cooperation between political and private organizations to manage information in order to improve national security shouldn't be ruled out.

Furthermore statistical data must be taken into consideration; this data can include illicit acts of interference against aviation, growth trends in the transportation of travelers, number of bomb threats by phone on airlines, and other types of threats against aviation, etc.

To assess threats, different data collection systems must be considered, such as:

Reporting incidents and other events: The relevant authority should have a methodology allowing anybody to submit an anonymous or voluntary report, as well as those that are required by law and must be submitted to the relevant authorities. Therefore it must be ensured that the system is user-friendly, quick and secured to protect and manage information, as well as the confidentiality of the information of the person submitting the anonymous or volunteer report.

Investigation of AVSEC Incidents / Events: It is important to obtain from any incident investigation related to illicit acts of interference, the information that will allow us to identify the underlying threats that caused the event, such as security weaknesses that lead to the incident. All this data is necessary for the implementation of appropriate countermeasure, as well as to provide data to identify new trends and/or emerging threats when assessing risks.

Data collector: Considering that many relevant authorities cannot assign AVSEC inspectors to all the airports of the State, it would be of great help to have technical staff properly trained (for example: air traffic controllers, government inspectors from different areas such as operations, AGA and airworthiness located at the airports, etc.). The trained staff, in cooperation with the relevant authority, could fulfill the mission of collecting information useful to the AVSEC inspectors, who can-after analyze and classify said data-launch investigations or facilitate concrete risk assessments.

The staff assigned to collect information should be carefully selected and trained, as well as to have the necessary resources to guarantee that the information being transmitted is protected from any unwanted interference.

State's Security Agency: A key factor in the risk assessment process is the permanent participation from different government security agencies to provide the information that relevant authorities need to identify threats according to the reality of each State. Therefore, it is necessary to setup work procedures to guarantee the appropriate level of confidentiality to the information provided by security and intelligence agencies, to avoid information leaks that can put at risk the operational and preventive security measures.

Other sources of information: It is important to have access to difference sources of information allowing the personnel in charge of risks assessment to identify suspicious trends or behavior at airports, facilities, operations by air carriers, or any other activity related to the aviation industry of the States.

In addition, other important sources of information are specialized services by subscription, providing detailed summaries of events taking place in other parts of the world. These reports can be helpful when assessing risks for international aircraft operators flying from different regions to the State's airports.

However, to provide a risk assessment to the relevant authorities responsible for implementing airport security decisions, the information must be up-to-date and reliable, thus the need to use multiple data sources. Since it is difficult to find reliable information on threats against aviation, the analysis process should not rule out sporadic and vague information available nor the assistance of staff specialized in detecting needs for information, and translating such needs into real requirements satisfied through open sources of information or technological means. All this in order to balance global needs, basic intelligence and the non-realization of the latter through specific requirements.

Lastly, the data collection systems shall provide important information that could be used by the analysts to identify, and consider the potential threats to the aviation industry, to adapt countermeasures needed to counteract the incidence of illicit acts of interference. Once the threats are identified, this information is completed with detected vulnerabilities in the security study for each airport, or airline, which would allow to set the risk level in which the assessed company operates (applying the following formula: Threat x Vulnerability = Risk).

Analysis and Generation of information

The analysis is the backbone of identifying threats, and the key to reaching efficient, relevant, and timely results. When a threat assessment is carried out, the analysis is the crucial phase that will allow the application of all intellectual capacities.

Currently, analysis is the fundamental tool used in intelligence, and it will continue to be in the future. The key for all the information to make sense, that it is understandable and to facilitate decision-making to those responsible based on past and current events, is to consider the following questions: why things happen, and how will they take place in the future. This is highly relevant since most civil aviation organizations have limited resources, therefore the analyst(s) should consider only pertinent objective data instead of subjective speculation.

Is important to assure that during the threat analysis, the analyst(s) avoid(s) the influence of any institutional regulations such as attitudes or habits that an organization may perpetuate as established regulations that could prevent a well thought-out process. The analyst should try to limit himself or herself to make use of traditional methods or processes; he/she should incorporate traditional thinking into innovating assessment techniques.

The analyst of this type of information, whether he/she is a well-trained specialist on information services, law enforcement agent or aviation security professional, must assess data systematically. At this point the analyst is applying the principle one to identify threats, while the other two principles plan an important role in the risk management process.

Assessing the data source in terms of its usefulness, credibility, opportunity, accuracy, and its integration will contribute in a positive manner to the implementation of the information requirements previously established in the initial phase, for their relevance and usefulness based in two criteria: source validity, and information relevance.

Source Assessment		**Information Relevance**	
A	**Very reliable**	**1**	**Positive**
B	**Generally reliable**	**2**	**Probable**
C	**Reliability unknown**	**3**	**Uncertain**
D	**No assessment**	**4**	**No assessment**

Establishing the treat and vulnerability criteria

The analyst(s) must determine first the threat and the vulnerability criteria before the assessment, deciding which ones will be the concentration points and “gravity centers” defining them by factors or criteria according to their importance and value as objectives or targets, for example:

- An airport,
- An air operator,
- A specific aircraft or
- A group of people.

The analyst(s) should take into account that an illicit act of interference against civil aviation is premeditated and carried out by criminals with an end, thus planned. Therefore, before assessing the way an illicit act of interference could be carried out against a specific target, the motives of such act against civil aviation and the probability of being perpetrated should the considered.

The analysis must create a work instrument for the evaluation process known as "vulnerability matrix', which will allow – using a methodology- establish a monitoring process for a group that could represent a threat to aviation. In addition, it will carry out the risk management process and assess the vulnerabilities of the airport.

Profile of groups (See Annex "A")

For a profile of a group vulnerabilities matrix, we must assume that most of the "anthropogenic systems" can be organized based on 5 basic characteristics. Therefore, any groups can be defined according to the following components: leadership, essence of the system, infrastructure, population, and combat mechanism. These five components will become the gravity centers for the assessment of a group with the potential of perpetrating illicit acts of interference – terrorist group, insurgent faction, or an organized criminal group.

- **Leadership:** The group's hierarchy, presence of legitimate political representation, use of charismatic individuals, just to name a few.

- **Will and means:** Of the group to implement their theoretical goals, such as political programs, or religious causes, through surveillance operations, acquisition of weapons, development of financing sources and training of their agents.

- **Infrastructure:** Combines several elements, such as magnitude, number of "cells" or subunits of the groups, established communication network, and an effective use of transportation and supply channels.

- **Support from the population:** made up by local supporters or others that could provide a safe heaven, food, and money to the group, because they are in agreement with their objectives, or possibly afraid or by coercion.

- **Combat mechanisms:** Capacity to carry out actions by the group to reach their goals. Members of said group could be identified as "combatants", for example, air pirates or "technical" such as those who put together bombs.

Without prejudice to the previously mentioned elements, other secondary functional categories could be mentioned depending on the level of the depth of the analysis requested by the analysts. These secondary categories can include:

- Capability of a group to commit violent actions.
- Location and background of previous activities.
- Level of commitment to their ideological ends (in other words, suicide attacks by individuals carrying bombs).

Based on the matrix results, the analysts will have the group's profile and a reliable understanding of their capabilities in terms of committing an illicit act of interference against civil aviation. Finally a respective report will be submitted to the relevant authorities for its diffusion.

Diffusion

The diffusion does not only mean submitting the final product to the requesting entity or intelligence consumer. There is a value added effort that includes the understanding and permanent urgency that civil aviation or airport authorities have to implement their measures, considering awareness, air carriers, airport terminal authorities, and others.

This phase entails distributing and making the final product available to the relevant authorities of civil aviation. The final product refers to the threat assessment, which must meet the following principles:

- Opportunity: Essential, provided at the precise moment
- Accessibility: For decision-makers
- Objectivity: With greater possible precision to avoid errors in the decision-making process
- Security classification: Confidential, Secret or Top Secret as appropriate.
- Communication: Establish a system to transmit information in a timely and secure fashion

The satisfaction with the final result: this traditional matrix should not be stagnant; on the contrary it requires to be dynamic and to permanently reassess the results and lessons learned. With the understanding that assessing any threat provided by intelligence must flow quickly at all levels — horizontally and not necessarily vertically or hierarchically— to boost the direct and effective application of the security measures.

The final intelligence data should be submitted by the relevant organization to the aviation authority using the following threat levels:

Low Threat Level: There is a low probability of an illicit interference occurring, no damages are expected, and normal security conditions should be maintain.

Medium Threat Level: There is a medium probability of an illicit interference occurring, with medium damages, thus special security measures must be enforced.

High Threat Level: There is a high probability of an illicit interference occurring, with major damages, thus extreme security measures must be enforced.

CHAPTER III

Risk Management

Annex 17 requires each contracting State to constantly keep under examination the level of threat against civil aviation in their territory, and to establish and apply policies and procedures to adjust as a consequence the pertinent aspects of their National Security Civil Aviation Program (NSCAP). This requirement has to do with two concepts – threat assessment, and risk management; together they are the basis for a viable and efficient response in line with the cost of illicit acts of interference in civil aviation.

The contracting state shall appoint the entity responsible for the threat assessment, and the aviation or civil aviation authority as the responsible entity for risk management. However, three key security principles must be considered: **identification, application and maintainance.**

When assessing threats, the first principle applies. While the second and third principles play an important role in the risk management process.

In terms of airport security, the third principle (maintenance) applies, which refers to the will and capacity to maintain a suitable and reliable security system. As well as when these phases are adopted to prevent illicit acts of interference and other criminal activities against airports and air carriers, and that must be verified through the National Civil Aviation Security Quality Control Program (NCASQCP).

A risk can be defined as the exposure to the probability of a successful attack occurring against a target. The concept of risk has two elements: probability of something occurring, and the severity, if it occurs.

- What is the probability of an illicit interference occurring?
- What would the severity of the damages be if an illicit interference occurred?

Risk Management must be a logical and systematical process that can be used to make decisions in security systems at the airports.

Aviation authorities must ensure Director or security officers at airports (as part of risk management) apply policies, procedures systematically, and measures to identify, analyze, assess, treat and control risks in order to be prepared.

Risk Analysis
In this step, airport authorities must analyze the probability and severity of each risk factor to determine the risk level considering the following two aspects regarding current controls.

For this matter, external and internal factors that could impact airport security must be considered, and some indicators can be used to detect or identify risks such as:

- Results of the airport security study
- Intelligence data with the threat level to the airport

- Intelligence data with the threat level of an air carrier;
- Feedback from security audits at the airport;
- Feedback from security audits at the airport for air carriers;
- Feedback of security inspections of security procedures at the airport;
- Feedback of security inspections of security procedures for air carriers;
- Results of security tests carried out of the security systems at the airports;
- Percentage of lost or stolen airport IDs;
- Information provided by security Directors or Managers from the air carrier's data bases related to staff turnover, labor conflicts, etc.
- Information provided by police related to common crimes committed at airports;
- Learn about the configuration and operations at the impacted facilities;
- Carry out an inventory of personnel, and security team available;
- Examine the current security measures;
- Assess the number of flights, passengers, and the luggage and cargo volume that would be subjected to improved security procedures;
- Security investigations as a result of a report by a passenger, crew member or an airport user.

Moreover, other aspects or conditions that promote or prevent the incidence of a threat should also be taken into account, such as:

- Geographical location of airport (rural or urban context)
- Airport fencing infrastructure or boundary fences
- Status of lighting in the different areas of the airport
- Current security technology
- Current communication resources
- Access roads to and from the airport
- Adjacent land and neighbors
- Infrastructure, terminal building for passengers, cargo and more
- Airport security staff

Risks Matrix for Airport Risk Management (See Annex "B")

This is a practical instrument that reflects the status or level of procedures, infrastructure, staff, and threats among others elements raised and analyzed by the airport security authority.

The selected indicators and the level assessment of each one will allow to know the probability of incidence, and actions or measures to be taken prioritizing the most vulnerable to prevent potential illicit interference.

The results of this risks matrix will be determined as follows.

- **High Risk:** Requires implementation of immediate security measures and actions to increase it to a superior level.
- **Medium Risk:** Requires measures and attention at the airport level.
- **Low Risk:** It's handled through routine procedures.

Level of Impact

The result of the Risk matrix should not determine the impact level (severity of damages, major, moderate or low) to the security of civil aviation, possibly affecting human lives, damaging an aircraft or paralyzing, for a period of time, airport operations.

- **Major 3:** Risk that would **SIGNIFICANTLY** damage the normal development of civil aviation activities to transport passengers and cargo.
- **Moderate 2:** Risk that would cause **MINOR** damages in the development of civil aviation activities to transport passengers and cargo.
- **Lower 1:** Risk that would have a MINIMAL effect on the development of civil aviation activities to transport passengers and cargo.

This risk matrix should be dynamic and must be updated frequently. It can be used as a working tool, allowing intelligent forecasting management for the decision-making process, facilitating a better and more efficient management to security personnel, and avoiding the application of more intense preventive measures linked to the major threat level with expenditures that represent a heavy financial burden to the aviation authority. Therefore is more efficient to deploy defense mechanisms where and when needed instead of applying them everywhere. This concept allows risk management.

CHAPTER IV

Airport Alert Status and Responses

Airport alert statuses are the result of the threat evaluation and risk management, and their purpose is to prevent subsequent illicit acts of interference against civil aviation. The aviation or civil aviation authorities must establish mechanisms to determine the airport **Alert Statuses** in the country. During said statuses, it will be necessary to increase security measures and implement at the same time additional protection activities aimed at reducing the vulnerability of airport activities and increase at the same time the capacity to response to incidents.

According to the risk, three (3) alert statuses must be defined, identified by color of universal knowledge, and easy to understand by those in charge of implementing airport security measures, the established colors for alerts are:

- **Green alert/Low risk**
- **Yellow alert/Medium risk**
- **Red alert/High risk**

These Alert Statuses shall be established on a permanent basis at the airport(s) changing in accordance with the notice reported by the authorities that are based on the threat assessment and risk management. The measures and countermeasures to be implemented shall be according to the alert status notified:

Green Alert: Indicates low threat conditions, according to the intelligence available, an air carrier or airport is not considered target to an attack; however, there is still the possibility of illicit interference by a people or a group, due to causes like civil demonstrations, labor conflicts and the active presence of groups opposed to the government.

Yellow Alert: Intelligence indicates that there is a probability that one or more air carriers will be targets of an attack, in addition other background information should be considered such as:

- At the request by another State to implement special security measures.
- Reporting of wrong information that may compromise the security of an aircraft in flight, on land or the safety of the passengers, crew, land personnel, and public in an airfield or building of civil aviation facilities.
- Increase of number of airport IDs lost
- Failure detected of an air carrier’s security system
- Labor conflict, strike by the personnel of an air carrier or airport terminal

Red Alert: The intelligence indicates one or more air carriers or airports are real targets of an attack. Nevertheless, this alert can also be activated under the following circumstances:

- Bomb threat (explosive artifact) in an aircraft;
- If there are justified suspicions that an aircraft will be attacked on land, according to the National Security Program;
- When learning that an aircraft in flight has been seized illegally.

"ANNEX "A"

Threat assessment table according to the group profile

Criteria and values of the attribute of the threat assessment system representing the group profile

Name of the group being assessed:_____

Caption

Total points 11 – 15	=	**High Probability/High Risk** of this group committing an illicit act.
Total points 6 – 10	=	**Medium Probability/Medium Risk** of this group committing an illicit act.
Total points 0 – 5	=	**Low Probability/Low Risk** of this group committing an illicit act.

ATTRIBUTES	CRITERIA	VALUES	POINTS
LEADERSHIP	Does the group have a leader?		
	Is it centralized?		
	Is it united around its objectives?		
ESSENSE OF THE SYSTEM	Does the group have a cause or motive?		
	Have they made the cause public?		
	Is the group sufficiently able to act?		
INFRASTRUCTURE	Does the group have a known structure?		
	Is it a broad structure?		
	Is it efficient?		
POPULATION	Has the group received support from local or foreign government sources?		
	Does the group have local supporters?		
	Are the group members enthusiastic?		
COMBAT MECHANISM	Does the group recruit members actively?		
	Do members receive operation training?		
	Has the group carried out successful attacks?		
		TOTAL POINTS	
		ESTATUS	

"**ANNEX "B"**

I. Methodology for the implementation of the risk matrix

1. This progress begins with the identification of the "components" of civil aviation security, and the requirement for the efficient development of such components. Matrix on **ANNEX C** can be used as an example.
2. The specific inherent "risks" for each component that could affect its development, are identified.
3. Next step is to determine the incidence "probability" of the risk.
4. Then the potential "level of impact" is determined, which will be generated by the incidence of the risk over the "component".
5. Subsequently, "the risk level" is determined, based on the "probability" and the "level of impact".
6. Finally, the best actions to control, eliminate, and/or mitigate the risk, according to the probability, level of impact and risk level.

II. Specific components of the risk matrix

a) Security components

The essential elements or resources needed in airfields for the security of civil aviation.

b) Requirement of components

It is the most optimal condition of the component to provide security for civil aviation.

c) Specific risk

Adverse events that can affect the development of the component and its requirements.

d) Incidence probability

Possibility of a specific risk taking place, express in qualitative and quantitative values according to the table below.

INCIDENCE PROBABILITY	VALUE	DESCRIPTION
PROBABLE	**3**	Incidence **HIGH than** the current risk.
MODERATE	**2**	Incidence **MEDIUM than** the current risk.
UNLIKELY	**1**	Incidence **LOW than** the current risk.

e) Impact level

It is the consequence or damage level related to the incidence probability of the risk, expressed in qualitative and quantitative values according to the table below.

IMPACT LEVEL	VALUE	DESCRIPTION
GREATER	**3**	Risk that would affect **SIGNIFICANTLY** the development of the component and its requirement; and the fulfillment of its functions, preventing its normal development.
MODERATE	**2**	Risk that would have a **MINOR** effect in the development of the component and its requirement; making it difficult or delaying the fulfillment of its functions, preventing its normal development.
MINOR	**1**	Risk that would have a **MINIMAL** effect in the development of the component and its requirement; and does not affect the fulfillment of its functions.

f) Risk Level

It is the product between the "incidence" and the "level of impact", expressed in quantitative values for a specific component, compared to a defined standard according to the following table.

.

RISK LEVEL	VALUE	
Between 07 and 09	**3**	**HIGH**
Between 04 and 06	**2**	**MEDIUM**
Between 01 and 03	**1**	**LOW**

g) Actions to mitigate risks

Most appropriate actions or measures that must be implemented to control, eliminate, and/or mitigate risk. (**ANNEX C**)

h) Justification

Refers to the justification by local authorities when the risk level is **MEDIUM** and/or **HIGH**.

i) Security level

Is the sum of the "Level of Risk" of all the components of the security system, compared to a minimum standard defined in the following table.

∑ OF RISK LEVEL	SECURITY LEVEL	SECURITY CONDITION
Between 030 - 090	**4**	**OPTIMAL**
Between 091 - 150	**3**	**GOOD**
Between 151 - 210	**2**	**REGULAR**
Between211 - 270	**1**	**DEFFICIENT**

SECURITY CONDITION	SECURITY LEVEL	DESCRIPTION
OPTIMAL	**4**	Indicates an “optimal” condition of the security level of the airfield, with no risks in the security components.
GOOD	**3**	Indicates a “good” condition of the security level of the airfield, with minor risks in the security components.
REGULAR	**2**	Indicates a “regular” condition of the security level of the airfield, with greater risks in the security components.
DEFICIENT	**1**	Indicates a “deficient” condition of the security level of the airfield, with extreme risks in the security components.

III. General provisions to complete the matrix.

A. Common to all Components

The airport authority, should appoint the organization responsible for completing the risk matrix, the **measuring period**, and for that task, the following actions shall be carried out:

1. There is no password to open the Excel file; however, the user of each State can protect the file using these measures.

2. Select “**Airport**” from the dropdown list.

3. Select “**measuring period**” from the dropdown list.

4. Select the “**year**” from the dropdown list.

5. Go to the cells on the column titled “**Incidence**”; click the cell, and select the dropdown list for probability of incidence (**PROBABLE /MODERATE /UNLIKELY**); generating automatically the quantitative value assigned according to the table in previous section d).

6. Go to the cells on the column titled “**Level of Impact**”; click the cell, and select the dropdown list for Level of Impact ((**MAJOR/ MODERATE / MENOR**); generating automatically the quantitative value assigned according to the table in previous section e).

7. Subsequently in the columns titled “**Level of Risk**” the level of risk will automatically be displayed, resulting from the product between “Incidence” and the “Level of Impact”, according to the table in previous section f).

8. In the following column titled "**Risk Mitigation**", the actions to implement in the airfield will automatically be displayed, in order to control, reduce or eliminate the incidence or effects of the specific risks.

9. When the "Risk Level" is MEDIUM and/or HIGH, the reasons for these levels must be briefly entered in the "**Justification**" column.

10. At the end of the table, on the "**Level of Security**" cell, the security level of the unit will be automatically displayed, as a result of the automatic sum of all the values for each Risk Level. This is based on a defined standard expressed in a qualitative and quantitative value, according to the previous table in section i).

IV. Instructions for those responsible of the risk matrix

1. Those responsible of the AVSEC Risk Matrix should maintain it up-to-date on a permanent basis.

2. The risk or threat facts that could affect some of the Security Components should be taken into account, such as: **high-risk flights; notification of threats from other states; and threat levels notified by relevant state authorities**; which will determine the "Incidence" and the "Level of Impact", reporting the information to the respective airports or airport authorities so that those responsible enter the assigned qualitative values in the Risk Matrix.

3. The components previously mentioned, shall maintain the initial qualitative values; and will only vary when the aviation or civil aviation authorities report a new value for "Incidence" and "Level of Impact".

SAMPLE OF MANAGEMENT MATRIX

	SECURITY COMPONENTS	COMPONENT REQUIREMENT	SPECIFIC RISK	INCIDENCE		LEVEL OF IMPACT		RISK LEVEL		MITIGATION OF RISK	JUSTIFICATION
1	Limits between the public area and the airfields. .	Establish the limi between the public and the airfield areas.	Deficient security management in the areas o coordination and implementation.		0		0				
2	Restricted security areas	Enough personnel to carry out al functions.	Deficient execution of the different security functions.		0		0				
3	Screening of passengers (if centralized)	PSA updated approved and diffused.	Does not have local security measures o applies out of date measures.		0		0				

Note: The Risk Matrix is attached as an Excel file

ANNEX "C"
Proposed security measures based on the security alert statuses

N	Security Component	Green/ Risk Low (basic measures)	Yellow/Risk Medium (intermediate measures)	Red/Risk High (high measures)
1	Limits between the public and airfield areas. .	Establish limits in the aviation section. Protect, screen, and control all access through the limits to irregular intervals.	Apply basic measures, and more surveillance and patrols. .	Apply intermediate measures. .
2	Security restricted areas	Control access to security areas at all times. Use a pass system and other means for vehicles, staff and crews. Verify all IDs, and passes at the access points. Screen vehicles and supplies randomly.	Apply basic measures, and inspection of at least 20% of the staff, items transported, and vehicles before allowing access.	Apply basic measures, and inspection of at least 100% of the staff, items transported, and vehicles before allowing access.
3a	Screening of passengers (if centralized)	Manually screen all passengers with metal detection equipment before allowing access to the security restricted area.	Apply basic measures, and manually screen 10% of all passengers at the gate.	Screen all departing passengers manually at the departure gate or manually screen all passengers with metal detection equipment before departure. Manually screen 20% of passages screened with metal detection equipment.
3b	Screening of passengers (at the gate)	Same as 3a.	Same as 3a.	Same as 3a.
4a	Screening of carry-ons (if centralized)	Screen all carry-ons from departing passengers, manually or with X-ray equipment. Ten percent of carry-ons screened with X-ray machines must be manually screened.	Apply basic measures and manual screening of 10% of carry-ons (or with approved modern technology) at the departing gate. .	Screen once again carry-ons of all departing passengers leaving the departure gate, manually or with X-ray machines before departure. Manually screen 20% of carry-ons (or with modern technology that has been approved) that were screened with X-ray machines.
4b	Screening of carry-ons (at the gate)	Same as 4a.	Same as 4a.	Same as 4a.

N	Security Component	Green/ Risk Low (basic measures)	Yellow/Risk Medium (intermediate measures)	Red/Risk High (high measures)
5	Separation of screened and non-screened passengers. .	Separate passengers that have been screened from those entering. When physical separation is not possible, apply compensatory measures in accordance with the threat assessment carried out by the national authority.	Apply basic measures.	Apply basic measures, increase surveillance of the compensatory measure.
6	Verification and security screening of the aircraft.	Verify/screen aircrafts (when start operating) before departure, and aircrafts in transit to ensure that no weapons, explosives or dangerous artifacts have been left on board.	Apply basic measures.	Carry out a complete security inspection of the aircraft with the assistance of appropriate detection, at the discretion of the relevant authority.
7	Control to access the aircraft.	Restrict access to the aircraft to authorized personnel with onboard tasks, and passengers. The doors should be shut closed, and steps removed if the aircraft is not under surveillance or the airbridges have been withdrawn.	Apply basic measures.	Strict control of access to aircraft with guards in each gate used. All personnel trying to access must be subject to manual screening as well as their belongings.
8	Risk assessment of passengers.	No requirements.	No requirements.	Subject all passengers to the risk assessment system, and certain passengers to a more strict screening.
9	Compare against records the checked-in luggage.	Compare against records checked-in crew and passengers luggage before loading, through manual or automated channels. All non-accompanied baggage must be identified.	Apply basic measures.	Apply basic measures or positive identification of passengers or cargo. .

N	Security Component	Green/ Risk Low (basic measures)	Yellow/Risk Medium (intermediate measures)	Red/Risk High (high measures)
10	Screening of checked-in luggage	100% screening of all checked-in luggage of origin and transfer, by hand, traditional X-ray machine or explosive detection system (EDS). Regarding the transfer of checked-in luggage, an exception could be made when there is an on-going validation and application system in place for screening procedures in the point of origin, and when the luggage is subsequently protected from non-authorized interferences from the airport of origin to the aircrafts departing from the transfer airport.	Apply basic measures, and when X-ray machines are used, must also screen 10% of luggage manually or using modern X-ray technology.	Apply intermediate measures to use the best technology and the best available procedures.
11	Checked-in luggage not accompanied.	Screen all checked-in luggage, not accompanied, except with the origin and ownership can be verified. .	Screen all not accompanied luggage, manually or with explosive detection equipment, or subject the luggage to an air simulation using a compression chamber or not transport it	Apply intermediate measures.
12	Protection of checked in luggage	Protect checked-in luggage from non-authorized interference from the point of inspection or receipt, from both the first one, all the way to the aircraft departure. If the integrity of checked-in luggage were threatened, it must be screened before loading on to the aircraft.	Apply basic measures.	Apply basic measures and keep checked-in luggage under constant surveillance by security guards assigned to the task, or transport it in sealed containers, tamper proof, and verify it.
13	Air cargo	Submit all items to security controls of air carriers or from the appointed regulated agents or any relevant authority before loading them up into the aircraft.	Apply basic measures with a new random screening, and additional verifications (except for regulated agents)	Submit all items to security controls or a full on flight simulation protecting even the cargo. Intermediate measures should apply to aircrafts transporting only cargo.

N	Security Component	Green/ Risk Low (basic measures)	Yellow/Risk Medium (intermediate measures)	Red/Risk High (high measures)
14	Protection of air cargo	Submit all items to security controls of air carriers or from the appointed regulated agents or any relevant authority before loading them up into the aircraft.	Apply basic measures.	Apply basic measures and keep cargo under constant surveillance by security guards assigned to the task, or transport it in sealed, tamper proof, containers and verify it.
15	Mail	Submit all items to security controls of air carriers or from the appointed regulated agents or any relevant authority before loading them up into the aircraft.	Apply basic measures with new random screening and more verifications (except for regulated agents).	Screen all mail or submit to a flight simulation in a compression chamber and protect it until it is loaded. Intermediate measures should apply to aircrafts transporting only cargo.
16	Protection of mail	Protect the mail against non-authorized interference from the point where security controls are applied Until the departure of the aircraft. .	Apply basic measures.	Apply basic measures and keep cargo under constant surveillance by security guards assigned to the task, or transport it in sealed, tamper proof containers, and verify it.
17	Items for services and flight and supplies	Submit all items to security controls to prevent the introduction of banned items in flight service items and the supplies that are loaded on the aircraft, and protect them until they are loaded unto the aircraft.	Screen a reasonable percentage of in-flight items and supplies, and escort them to the aircraft or transport them in sealed, tamper proof containers.	Prepare all service items for flight and supplies under the direct security supervision of the air carrier or screen them before loading, and escort them all the way to the aircraft or send them sealed.
18	Appointed security coordinator	No requirements.	No requirements.	Appoint a special security coordinator to ensure that all measures have been applied correctly.

— END —