RWANDA AIRPORTS COMPANY

AIR NAVIGATION SERVICES

SECURITY PROGRAM

Doc. No.	Issue No:	Revision No:
RAC-KIA-ANS-SeCP002	01	01

DOCUMENT IDENTIFICATION

KIGALI INTERNATIONAL AIRPORT

Issue Date:	May 2018
Reference No.	RAC-ANS-SeCP002
Title	Air Navigation Services Security Programme

RECORD OF AMENDMENT

a. Amendments to this manual will be done by the Director, Air Navigation Services. Whenever a need arises for an amendment, the Director Air Navigation Services will submit the proposed amendment to the Director General/Rwanda Civil Aviation Authority for approval through the Managing Director. Upon approval, amendments to this manual are made by means of replacement sheets. When the replacement sheets have been inserted, and the replaced sheets removed, an entry will be made in the table below.

b. The ANSP shall implement all the directives, instructions, orders and circulars as provided by Rwanda Civil Aviation Authority.

No.	Date Applicable	Date Entered	Entered by
1	May 2018		

LIST OF EFFECTIVE PAGES

Page	Date	Page	Date	Page	Date	Page	Date	Page	Date	Page	Date
1	May 2018	8	May 2018	15	May 2018	22	May 2018				
2	May 2018	9	May 2018	16	May 2018	23	May 2018				

3	May 2018	10	May 2018	17	May 2018	24	May 2018				
4	May 2018	11	May 2018	18	May 2018	22	May 2018				
5	May 2018	12	May 2018	19	May 2018	23	May 2018				
6	May 2018	13	May 2018	20	May 2018	24	May 2018				
7	May 2018	14	May 2018	21	May 2018	25	May 2018				

MANUAL DISTRIBUTION LIST

S/No	Title	Organization	UNIT/DEPARTMENT
01	Director General	RCAA	DG
02	Managing Director	RAC	MD/RAC
03	Deputy Managing Director	RAC	DMD/RAC
04	Director Airport Unit	RAC	DAU
05	Director Flight Safety Standards	RCAA	DFSS
06	D/ANS	RAC	ANS
07	C/ATC	RAC	ATC
08	AVESC Inspector	RCAA	
09	AVSEC Airport Operation		
10	D/FSS-LIBRARY	RCAA	FSS
11	KIA TOWER	RAC	ATC
12	KIA APPROACH	RAC	ATC
13	SAFETY MANAGER	RAC	ANS

FOREWORD

This Security programme document was developed by Air Navigation Services (ANS) Directorate with the intention of providing ANS employees and authorized security personnel proper processes and procedures that will meet a universally accepted level of security.

The Security Programme is a collaborative security situation management capability for air navigation services in formulating the mechanism of a threat prediction capability to provide secure and reliable Air Navigation Service systems for a diverse set of applications or all acts of unlawful interference with civil aviation wherever they may occur.

Air Navigation Service integrated systems combining diverse applications may have some risks to the communication, navigation and surveillance/air traffic management (CNS/ATM) that could potentially increase vulnerabilities and make the system more prone to security attacks. There are several types of attacks on network communications such as disrupting or blocking communication, intercepting, interfering, accessing and modifying the information.

Although the emphasis in rulemaking has, to date, been on security for large airline aircraft and large airport terminals, it is also recognized that the Air Navigation Service has a role to play in a secure civil aviation system. In this program, the Security is applied to Air Navigation Service systems for identifying threats, assessing the risks involved, and defining measures to mitigate them. The risk assessment is performed to evaluate the impact and likelihood of occurrence of attacks relevant to the identified threats and the resulting risk levels. Consequently, specific mitigation measures are proposed to provide for the ANS integrated systems required high level security.

By implementing this ANS Security programme, ANS Directorate is intensifying efforts to eradicate such unlawful acts by complying fully with the specifications of Annex 17 to the Chicago Convention,

APPROVAL PAGE

Prepared on behalf of the:

Managing Director

Rwanda Airport Company

Sign……………………………………………………………………………

Name PASCAL NZARAMBA…………………………………………

Date 06 MAY 2018……………………………………………

RWANDA AIRPORTS COMPANY

Appoved by:

Director General,

Rwanda Civil Aviation Authority

Sign Silas Udahemuka……………………………………………

Name……………………………………………………………………………

Date 08 Aug 2018……………………………………………

RWANDA CIVIL AVIATION AUTHORITY
REPUBULIKA Y'U RWANDA
UBUMWE UMURIMO GUKUNDA IGIHUGU

Table of Content

IDENTIFICATION AND CONTROL

This document is identified as Air Navigation Services Security Programme (ANS SeCP)

Purpose of the document:
The purpose of this programme is to establish ANS Security Statement, responsibilities, procedures in general, and instructions for the security access control of ANS facilities, data and information and do not allow unauthorized access from outsiders.

Effective Date:
Effective date of an instruction is indicated at the foot of the page. New version will be indicated by date at the foot of the page.

Controlling the Manual
Directorate of Air navigation services will control this Manual electronically by maintain the master copy.
The Quality Manager (QM) is responsible for maintaining the process documents and forms in both
electronic and paper format and for ensuring their regular review.
ANS Managers are responsible for ensuring that employees comply with this programme.

References

- This manual should be read in conjunction with the following;
- ICAO Annex 17-
- Aviation Security Manual (Doc 8973 – Restricted)
- Civil Aviation Security Law Nº/2011 of 42/2011 of 31/10/2011 and;
- Civil Aviation (Security) Regulations

Enquiries
Enquiries / clarifications / suggestions, if any, should be addressed to:

The Directorate of Air navigation services,
Rwanda Airports Company
E-mail: ekaragire@rac.co.rw
Telephone: +250 724123150

Abbreviations

ATM: Air Traffic Management
ATC: Air Traffic Control
AFTN: Aeronautical Fixed Telecommunication Network
ARAP: Airport Restricted Area Permit
NCASP: National Civil Aviation Security Programme
ANS: Air Navigation ServicesASP: Airport Security Program
ATM: Air Traffic Management
ATS: Air Traffic Services
ATSP: Air Traffic Services Provider
CD: Compact Disc
CNS/ATM: Communication Navigation Surveillance Air Traffic Management
CMD: Control Monitoring Display
DBM: Data Base Management
DME: Distance Measurement Equipment
DRF: Data Record Facility
DVOR: Digital Very High Frequency OmniRange
ECM: Electronic Counter Measures
FDD: Flight Data Display
ILS: Instrument Landing System
MANSOP: Manual of Standards Of Procedures
MATS: Manual of Air Traffic Services
METAR: Meteorological aviation report
Navaids: Navigation aids
RCAA: Rwanda Civil Aviation Authority
RAC: Rwanda Airports Company
SDD: Surveillance Data Display
SPECI: Special observation.
SMS: Safety Management System
SOP: Standards Of Procedures
SSL: Secure Socket Layer
RF: Radio Frequency
RNP: Rwanda National Police
RDF: Rwanda Defense Force
VPN: Virtual private network

Explanation of Terms

Bomb Threat: A communicated threat, anonymous or otherwise, which suggests, or infers whether true or false that the safety of an aircraft in flight or on the ground, or any airport or civil aviation facility or any person may be in danger from an explosive or other item or device.

Compliance: Meeting the requirements of the NCASP and relevant approved aviation security programs.

Effectiveness: Extent to which planned activities are realized and planned results achieved.

Emergency Plan: A plan setting forth the procedures for coordinating the response of different aerodrome agencies or services and of those agencies in the surrounding community that could be of assistance in responding to an emergency.

Incident: Means any occurrence, other than an accident,

Permits: A permit system consists of cards or other documentation issued to individual persons employed on airports or, who otherwise, have need for authorized access to airport, airside or security restricted area. Its purpose is to identify the individual and facilitate access. Vehicle permits are issued and used for similar purposes to allow vehicular access. Permits are sometimes referred to as airport identity cards or ARAP.

Restricted Areas means those areas of the airside of an airport which are identified as priority risk areas where in addition to access control, other security controls are applied. Such areas will normally include, inter alia, all commercial aviation passenger departure areas between the screening checkpoint and the aircraft, the ramp, baggage make-up areas, including those where aircraft are being brought into service and screened baggage and cargo are present, cargo sheds, mail centers, airside catering and aircraft cleaning premises.

"Cyber security" encompasses the protection of electronic systems from malicious electronic attack and the means of dealing with the consequences of such attacks.

Restricted area access point means a point in a security barrier at which an access control system is in place that controls access to a restricted area from a non-restricted area

Screening: The application of technical or other means, which are intended to identify and/or detect weapons, explosives, or other dangerous devices, which may be used to commit an act of unlawful interference.

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

Security Control: A means by which the introduction of weapons, explosives or other dangerous devices, which may be utilized to commit an act of unlawful interference, can be prevented.

Security Program: The sum total of the legislation, policies, regulations, processes, procedures and measures ANS and other concerned stakeholders apply to help prevent unsecure incident to ANS facilities, systems and personnel.

Stakeholders: Airport tenants and other entities (regulated or otherwise), including industry associations with an interest in the aviation system.

Risk: refers to the likelihood of being targeted by a given attack.

Risk Management: The systematic and coordinated application of management practices aimed at identifying, understanding, assessing, acting on, monitoring, and communicating risk issues. Risk management provides a systematic approach to setting the best course of action under uncertainty.

Threat: Anything that has the potential to prevent or hinder the achievement of objectives or disrupts the processes that support them (i.e. an Act of Unlawful Interference).

Vulnerability: The effectiveness (or inadequacy) of security controls that could permit a threat to occur.

Impact: A combination of human losses, economic consequences, and political repercussions.

Resilience: The ability to resist, absorb, recover from or successfully adapt to, adversity or a change in conditions. • Security Value: The quantifiable impact or value of a certain security policy, measure, program, or technology

Hazard: Is a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.

Level of safety – degree of safety of a system, representing the quality of the system, safety-wise, expressed through safety indicators

Air Traffic Controller means the holder of a valid air traffic service license and valid rating which permits such holder to provide an air traffic control service

Jamming" or "Electronic Counter Measures" (ECM) is a term used to describe active means of trying to prevent the radar system from working as well as intended.

Air Traffic Service means an airport control service, an approach control service, an area control service, a flight information service, an air traffic advisory service or an alerting service

Air Traffic Service Unit means an air traffic service control unit, flight information centre or traffic service reporting office

Risk mitigation: The process of incorporating defences or preventive controls to lower the severity and /or likelihood of a hazard's projected consequences.

Security:

Physical Security: means providing environmental safeguards for controlling physical access to equipment and data on the ANS facility and network in order to protect asset and information technology resources from unauthorized use.

Finger protection for inner doors, i.e. devices which are mounted onto an existing inner door.

Availability A loss of availability is the disruption of access to or use of information or an information system. - "Ensuring timely and reliable access to and use of information…"

Risk Assessment is a process which determines what information resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Control Activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.

Authorization

Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Typically, authorization is performed in context of authentication. It is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify).

Privileged access

System administrators routinely require access to information resources to perform essential system administration functions critical to the continued operation of the organization. Such privileged access is often termed "superuser," "root," or "administrator" access. Privileged accounts enable vital system administration functions to be performed and are only to be used for authorized purposes.

Integrity

The assurance that arriving information is the same as what was sent out. Understanding integrity requires you to understand the concepts of data integrity and system integrity.

Confidentiality

The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and Secure Socket Layer (SSL) or virtual private network (VPN) connection helps ensure confidentiality when transmitting data across untrusted networks. Your security policy should conclude how you will provide confidentiality for information within your network as well as when information leaves your network.

Auditing security activities

Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access. Successful access records tell you who is doing what on your systems. Unsuccessful (denied) access records tell you either that someone is attempting to break your security or that someone is having difficulty accessing your system.

1. Introduction

The purpose of this programme is to establish ANS Security Statement, responsibilities, procedures in general, and instructions for the security access control of ANS facilities, data and information and in order to strengthen the security whether accessing or using ANS facilities by not allowing unauthorized access physically or logically.

Air Navigation Service systems have an integrated architecture of diverse radios, voice communication switches, routers, servers, switches, internet and associated control equipment with a separate remote control monitoring generally dedicated to each service. Combining various systems on the same infrastructure as well as integrating the many communication links, could potentially open up the ATM (Air Traffic Management) system to more attacks, thereby increasing vulnerabilities and the overall risk, unless adequate security measures are taken.

Therefore, the Security programme vision is to achieve secure and reliable communications between the external and the internal networks over a set of heterogeneous system links for a diverse set of applications, carried within multiple safety/security domains. In the programme, we have been looking at the security aspects of Air Navigation Service systems. For safety and security of the Air Navigation Service provision and its operations, all possible threats to the Air Navigation Service systems access and its operations must be identified, potential risks must be evaluated, and mitigations must be put in place through efficient implementation of security mechanisms.

These security mechanisms must implement and provide different security features to ensure that the Air Navigation Service system meets the security requirements.
The three main security requirements specified for consideration in information systems are to prevent unauthorized information disclosure (Confidentiality) and improper malicious modifications of information (Integrity), while ensuring access for authorized entities (Availability). There are several types of attacks on network communications including: disrupting or blocking communication, intercepting, injecting fabricated packets, accessing and modifying the storage, tables or packets.

Adequate security is a major expectation of the Air Navigation Service systems for the protection against threats that stem from intentional acts (e.g. terrorism) or unintentional acts (e.g. human error, natural disaster) affecting aircraft, people or installations on the ground.

2. Organizational and Personnel Responsibilities

The organizational and personnel responsibilities of Various Stakeholders related to the National Civil Aviation Security Program (NCASP), are covered under the Airport Security Program (ASP)

Refer to ASP Chapter 3 paragraph 3.1 through 3.1.22

Third-party personnel security

The National Civil Aviation Security Program (NCASP) shall establish personnel security requirements, including security roles and responsibilities for third-party providers (e.g., contractors, suppliers).

These requirements should be part of the selection criteria and must be satisfied by third-party providers. The Air Navigation Services shall also monitor provider compliance.

Examples of third-party providers include service bureaus, contractors (including maintenance contractors), and other organizations providing ICT system development, information technology services, outsourced applications, and network and security management.

Personnel sanctions

The RAC established and implemented a formal sanctions process for personnel failing to comply with established security policies and procedures. The sanctions process are consistent with applicable State laws, policies, and guidance. This sanctions process is part of the Air Navigation Services general personnel policies and procedures, and shall be described in access agreements.

Personnel support

The RAC should establish programmes for protecting and supporting employees and other persons with critical knowledge or functions. Examples include security awareness training, identifying and mitigating fear tactics used by terrorist and criminal agents and disaffected insiders, and offering protection and other resources for employees when they are threatened. The RAC should also train employees to help detect and counter insider threats by making management aware of suspicious or abnormal behavior and work practices of other employees.

3. Security Policy Statement

OBJECTIVE

The objective of Air Navigation Security Programme is to ensure the operation continuity of Air Navigation Service provision and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

POLICY STATEMENT

1. The Security Policy goal is to protect and secure the Air Navigation Services Systems and facilities against all threats internal or external, deliberate or accidental to ensure air navigation service provision continuity including access to aeronautical, meteorology and air traffic data information, guarantee the integrity and authenticity of records we hold, minimize operation damage and maximize return on investments and operations opportunities.
2. Data information is at the core of Air Navigation Services operations. It is the policy of ANS to ensure that:
   a. ANS security data information will be protected against any **unauthorized access**, **confidentiality** will be assured, **integrity & availability** will be maintained, and Availability of data information
   b. **Regulatory and legislative requirements** are meet;
   c. ANS staff are **trained in security management**;
   d. **All breaches and threats of data information security**, actual or suspected will be reported to the Director General;
   e. **Potential risks carefully** evaluated, and mitigations be put in place through efficient implementation of security mechanisms;
3. Detailed ANS procedure manuals support this policy. These include SMS manual on incident handling and reporting, badges wearing, access control, SMS risk asseessment and data information access and disposal.
4. The policy will be reviewed annually by the safety action group and review board.

RESPONSIBILITY

5. 1.1. The role and responsibility of the Director Air Navigation Services is to take the lead on ANS security program, to report to the Managing Director and to provide advice and guidance on implementation of this statement.

5.1.2. ANS Safety Manager is responsible for security routine liaison with law enforcement and Conducting evaluations. All ANS Departments Heads are directly responsible for implementing this Statement within their operation areas.

5.1.3. Each ANS Employee and any contractor working for ANS must adhere to this Statement.

3.1. Visitor control policy

5.2.1. The Air Navigation Services has established and implemented visitor control policies for visits by individuals or large groups to each type of ANS facility. The following procedure must be followed by visitor prior to being granted permission to visit ATC facility;

a) Being identified and registered by Airport Operations in charge
b) Acquiring authorization to access the facility from Airport operations office
c) Being escorted by authorized person/s
d) Leaving all photographic and recording devices with the first security checkpoint.
e) Signing agreement to protect information from access by unauthorized people
f) Holders of visitor security permits must be escorted at all times when within the Airside and SRA.

3.2. The National legal basis

This document has been developed in order to comply with the following national legal basis:
The National Civil Aviation Security Programme (NCASP) of Rwanda is given legal force by virtue of:

- Civil Aviation Security Law Nº/2011 of 42/2011 of 31/10/2011 and;
- Law No 21/2018 modifying law Nº/2011 of 42/2011 of 31/10/2011
- Civil Aviation (Security) Regulations

Additional legislation exists that supplements the provisions mentioned above. These are:

- The Civil Aviation Authority Law Nº42/2011 of 31/10/2011;
- Law Nº53/2011 of 14/12/2011 establishing the Rwanda Civil Aviation Authority (RCAA), and determining its mission, organization and functioning.
- Law N° 04/2011 of 21/03/2011 on immigration and emigration in Rwanda;
- Law N° 46/2010 of 14/12/2010 on the Establishment, General Organization and Jurisdiction of the National Police;
- Prime Minister's Order N° 123/03 of 30/04/2013 determining the responsibilities, organisation and functioning of a National Civil Aviation Security Committee;
- Prime Minister's Order N° 122/03 of 30/04/2013 determining the responsibilities, organisation and functioning of the Airport Security Committee;
- Organic law n° 01/2012/OL of 02/05/2012 instituting the penal code.

3.3. International Obligations

Because of the international nature of aviation, effective security requires the participation of all States. In order to achieve a uniform application of security provisions, several international legal instruments (conventions) have been developed. They provide the basis for the uniform implementation of security provisions worldwide.
The following conventions deal specifically with unlawful interference with Air navigation facilities:
a) The Convention on Offences and Certain Other Acts Committed On board Air navigation facilities (the Tokyo Convention), signed in Tokyo on 14 September 1963.
b) The Convention for the Suppression of Unlawful Seizure of Air navigation facilities (The Hague Convention), signed in The Hague on 14 October 1971.
c) The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (the Montreal Convention), signed in Montreal on 23 September 1971.
d) The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971, done at Montreal on 24 February 1988.
e) The Convention on the Marking of Plastic Explosives for the Purpose of Detection, done at Montreal on March 1991.
f) The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (the Beijing Convention), signed in Beijing on 10 September 2010.
g) The Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Air navigation facilities (the Beijing Protocol), signed in Beijing on 10 September 2010.

3.4. Other responsibilities

The Director Air Navigation Services is to take the lead on ANS data information security, to report to the Managing Director and to provide advice and guidance on implementation of this statement.
All ANS Departments Heads are directly responsible for implementing this Statement within their operation areas.
Each ANS Employee and any contractor working for ANS must adhere to this Statement.
Engineer automation systems administrator ensures that the facility computer and related equipment function properly. He also:
– Analyzes, logs, tracks and resolves software/hardware matters of significance pertaining to networking connectivity issues, printer, servers, and applications to meet mission needs.
– Coordinates hardware/software installations upgrades and monitors troubleshooting to ensure work is properly performed in accordance with established policy.
– Ensures changes are in accordance with appropriate operating procedures.
– Assists and advises controllers during emergencies.
–Evaluates the operational effectiveness of facility systems, subsystems, and security management.
Engineer Shift leader
– Ensure unique identification and assignment of access privileges

– Allow access to information resources only by authorized individuals
– Ensure periodic review of their authorized access rights • Maintain effective access mechanisms through evolving technologies

Chief Air Traffic Control will:
As soon as the ATC chief/facility receives notification of an accident or incident, he will
—Collecting and safe guarding data concerning aircraft mishaps, emergencies, or violations.
—Notify the chain of command. The notification will include
— Date and time of accident/incident. ν Number and type of aircraft involved.
—Number of injuries and/or fatalities.
—Brief synopsis of events to include ATC involvement.
—Actions taken.
— A point of contact by name, position, and telephone number to obtain additional information.
— Obtain a written statement about the incident or accident from all controllers and supervisory personnel involved. Written or taped records pertaining to an aircraft accident will be retained for a minimum of six months. Written or taped records pertaining to an aircraft incident will be retained for a minimum of 30 days.
—Request a local weather observation, unless there has been an intervening meteorological aviation report (METAR) or special observation (SPECI).
—Record all app if actual emergency situations require shutdown of these CNS facilities, he will immediately notify Director Air Navigation Services of the affected major facilities of the shutdown.

4. Air Traffic Management support for law enforcement

Whenever circumstances permit, as soon as practicable in advance of, or after an incidents or a contingency event has occurred, the Director Airport Operationshall convene the airport security committee established and published in the airport security programme. Its term of reference, administration arrangement and its composition are published in the airport security programme

4.1. Support law enforcement on specific operations and restrictions

Air traffic Management/RAC shall facilitate whenever requested by Law Enforcement Agencies (LEAs) to assist their operations through special handling of airspace and air traffic or provision of information related to specific flights operations such as police using helicopters and Remotely piloted aircrafts to stop or monitor an illegal activity on the ground or to support an enforcement operation against cross-border criminal activity.

4.2. Support law enforcement on airspace/flight restrictions

If security-related airspace/flight restrictions are needed, the ATM/RAC in coordination with the airport security committee normally chaired by the Managing Director shall establish a temporary airspace/flight restrictions. The dimensions and times of use of temporary airspace/flight restrictions shall be the minimum required for containing the expected activities, taking into consideration the safety requirements of the LEA air operations and regular flight operations.

In case of unlawful interference on-board an aircraft, or other illegal activity, ATM/RAC shall support LEAs in providing flight plan information on request, country of registry, operator, origin and destination and to detect and provide surveillance of aircraft suspected.

4.3. Support law enforcement on laser threats

If ATM/RAC receives an initial laser report from any pilot, he shall ensure that the following information is recorded:

a) time of the event;

b) aircraft ID;

c) aircraft type;

d) colour of laser (red or green, etc.);

e) position/location — fix/radial distance, approach to specific runway, nearest town, miles and direction from an airport, or latitude–longitude, etc.;

f) altitude;

g) aircraft's direction during the incident;

h) position of the laser in relation to the aircraft;

i) cockpit illuminated — Yes/No;

j) flight crew injuries — Yes/No;

k) flight crew visually hindered by visual effects (such as glare, flash blindness, loss of dark adaptation, glare discomfort and afterimage);

l) flight crew's intentions (e.g., continue/go around);

m) LEAs notified — Yes/No (name and phone number, if available);

n) brief description of the event; and

o) other pertinent information.

4.4. Support law enforcement on Man-Portable Air Defence System (MANPADS) threats

The ATM/RAC in coordination with the airport security committee normally chaired by the Managing Director shall create a strategic plan, procedures and determine alert levels response.

The ATC facility supervisor receiving the report or witnessing the attack shall ensure the information is communicated to the appropriate LEAs, airport security committee and civil authorities, as required.

4.5. Critical aviation information and communication technology systems

Further to the RCAA Advisory circular number 29-002, the RAC ANS Unit identifies the following as critical aviation information and communication technology data:

(a) Air traffic management data such as;
- Radar data
- Voice communication with aircraft and ground control
- AFTN
- Flight plans
- NOTAMS

(b) Met Data
(c) Any other data critical to the operations of the Aircraft

4.6. Protection of critical information data

(a) Administrative controls, such as:

- Access management
- Background investigations, selection criteria, and training of staff, particularly persons with administrator rights or those with the ability to access or modify sensitive and/or critical data;
- Segregation of duties, job rotation, separation of duties;

(b) Logical or technical controls, such as:
i) access control policies based on least privilege;
ii) firewalls and other security-related network components;
iii) data protection and encryption;
iv) data destruction according to policy;
v) malware and intrusion detection systems;
vi) anomaly detection systems;
vii) system end-point protection;

viii) network integrity;
ix) strong password policies;
x) log management policies and programmes;
xi) continuous patch management; and
xii) mobile device management;

(c) physical controls, such as:
i) ensuring data centers, communication facilities, and other spaces where hardware are located, are appropriately secured with limited access;
ii) physical access control systems using multi-factor authentication, biometric log-on methods;
iii) limiting the number of persons with authorized access and administrative privileges;
iv) contingency measures including the use of remote backup systems, in the event of loss of the primary system.
v) system maintenance are performed by authorized personnel only, and at prearranged and approved times. Number of persons authorized to provide support and maintenance of systems is limited to 2 people after conducting background checks with the National Police.
vi) Weekly inspection, testing of all critical infrastructure systems is conducted to ensure that access control is functioning properly and is able to withstand emergency situations.

5. Description of operations

In order to ensure the security and confidentiality of sensitive data & information while protecting against any anticipated threats or hazards, ANS has put in place all reasonable technological means, (i.e., security software, hardware) to keep information and facilities secure. The ANS Security programme has four main following components:

1. Measures related to access control;
2. Security response plan;
3. Physical and logical access authorization.
4. Navigation and vital facilities

5 1. Measures relating to ATM cyber security

Access controls can be both physical and logical, i.e. barriers that require a proximity card to gain access to the building are physical controls. ANS has rigorous access controls that are combined with proper authorization management – it is no use having access controls if a user can request access to a system and be granted access without proper approval, or if access is given before the approval is confirmed.

The following procedures for both physical and logical access will be done

5.1.1. Security Relevant Data Information and ATM Cyber Security

Cyber security could be an impediment to the implementation of the Global Air Navigation Plan. The term "cyber security" encompasses the protection of electronic systems from malicious electronic attack and the means of dealing with the consequences of such attacks. There are a number of assets, or components of the air navigation and air traffic system that need to be protected from threats and from becoming a threat.

Protective monitoring and physical access control are the two controls that will be part of cyber security mechanism to be used for people, processes and technology used for addressing cyber security issues.

a) People: measures related to physical access control including escorting engineers when in inspection should be enhanced
b) Processes: aeronautical information and meteorological data services will be protected, as well as the networks and technology handling the data and information using operating system like LUNIX not vulnable and digital access rights linked to a user account managed through active directory are logical controls.
c) Technology: The systems that collect, filter, process, create, store and distribute data and information are also prime assets susceptible to the cyber threat. This includes software, network protocols, computing algorithms, media storage

A lack of proper access controls can increase the likelihood of unauthorized individuals gaining access to areas that should be forbidden to them. This includes the following specific procedures:

5.1.1.1. Effective logging

□ When used? As long as the login window is displayed,

□ Who makes entries? The controller working position

□ What should be entered? He must enter the personnel user and password

□ What to do when entries have been made? If the login window disappears then the controller working position will start interact with the machine. If the login window reappears then the controller working position will notify the Engineer on duty for help and fixing it.

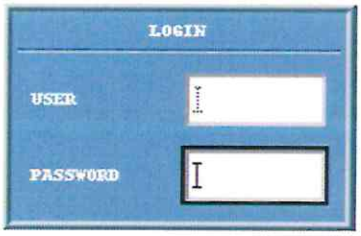
Each of the following equipment will need to enter correct user password for easy usage and unlock the control working position:

1. Operating system linux/unix which has greater security allowing to do almost

everything from the command line.

2. Main Processing equipment (servers: RDCU, SDP and FDP)
3. Operational controller working positions (SDD, FDD and CMD)
4. Auxiliary equipment (DRF,CTF and DBM)

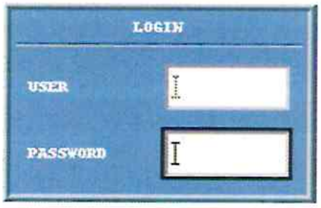
Surveillance Data Display (SDD): It has a LOGOUT Icon: End the current user session and display a window to enter the user and password for next operator. As long as this window is displayed, the System does not allow performing any action from this position but still displays all received data.



As shown in this figure, this window consists of two fields. The first one identifies the position's user and the second one is the password for entering.

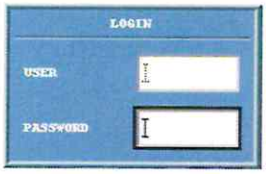
If the data are properly entered, when finishing, press <Enter> key and the action will be validated coming back the position to normal operation.

Flight Data Display (FDD):



This figure displays the "Login" Window to unlock the position. The first one is used to introduce user's code and the second to introduce the related password.

Control Monitoring Display (CMD):

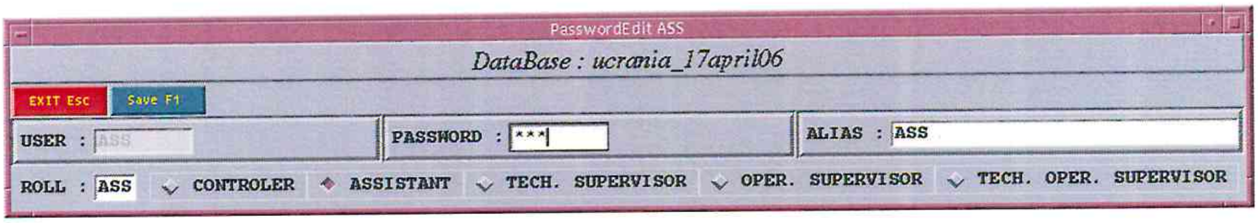


This figure displays the "Login" Window to unlock the position. The first one is used to introduce user's code and the second to introduce the related password.

Data Record Facility (DRF): Before starting the playback process, the corresponding SDD must be halted from the Supervision Position (CMD). Once it is not available (OFF in system mode), the controller starts up the playback function by introducing the Username and Password. The Username for the 24 hours playback is saved in DMS software.

Database Management System *(DBM):* The Database Management can be used to create different type of users and their corresponding passwords.

The User Password table contains information about the system users as well as the access keys to the controller's positions (SDD) and the role and responsibility related to each one. The table accepts up to two hundred fifteen (215) elements.



DataBase : ucrania_17april06

USER : ASS

PASSWORD : ***

ALIAS : ASS

ROLL : ASS ○ CONTROLER ● ASSISTANT ○ TECH. SUPERVISOR ○ OPER. SUPERVISOR ○ TECH. OPER. SUPERVISOR

User: User identifier.
Password: User password.
Alias: User alias.
Roll: It informs about the kind of role assigned.
Controllers: Work at a UCS.
Assistant: Works at a Flow & AFTN position.
S. Tec: Works as a technical supervision at a CMD.
Sup. Operative: Works as a controller supervisor at a CMD.
Sup Tec. Operative: Works as a controller supervisor at a CMD

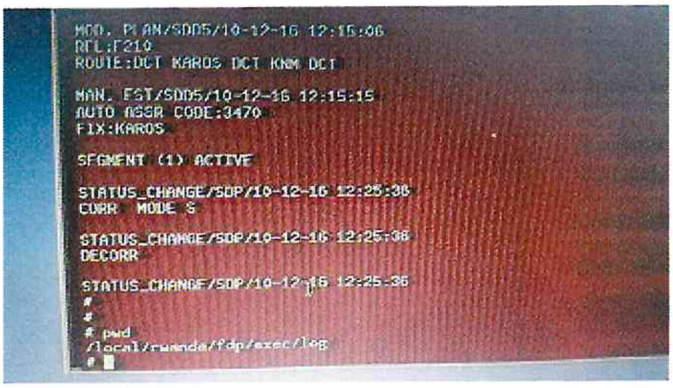
5.1.1.2. Effective Monitoring

All ANS equipment has built-in monitoring software and hardware to monitor the operating status of the CNS/ATM equipment as well as door access in DVOR/DME, ILS and Glide.

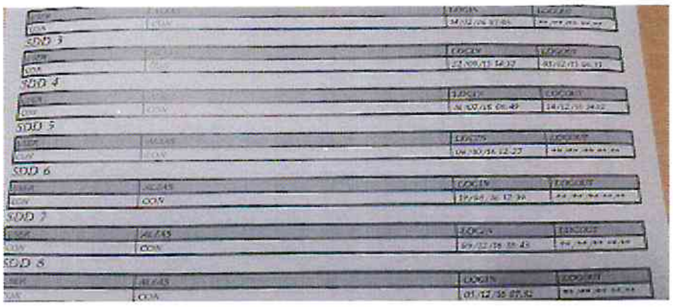
The Engineer must regulary check when on duty if there is no intrusion detection or threat monitoring system in place for the network, applications and DVOR/DME as well as ILS and Glide remote door access in order to know that it has been attacked; whether this is an external threat trying to breach the network from outside or an insider trying to gain access to systems they are not authorised to use. Other protective monitoring controls will be applied which could include an effective intrusion detection system.

This two pictures shows that:

- You can know which user is logged in and on which machine
- Know which machine did send what message.



```
MOD. PLAN/SDD5/10-12-16 12:15:06
RFL:F210
ROUTE:DCT KAROS DCT KNM DCT

MAN. EST/SDD5/10-12-16 12:15:15
AUTO ASSR CODE:3470
FIX:KAROS

SEGMENT (1) ACTIVE

STATUS_CHANGE/SDP/10-12-16 12:25:38
CORR  MODE S

STATUS_CHANGE/SDP/10-12-16 12:25:38
DECORR

STATUS_CHANGE/SDP/10-12-16 12:25:36
#
#
# pwd
/local/rwanda/fdp/exec/log
#
```


SDD 3
LOGIN
LOGOUT
SDD 4
SDD 5
SDD 6
ALIAS
CON
SDD 7
SDD 8

5.1.1.3. Effective Response Capability: In the case of any threat detected, the Engineer on duty will must act with the required speed and efficacy to report immediately the threat to his Chief for proper decision in this regards.

5.1.1.4. Equipment Disposal: Redundant information assets such as old hard drives, printers, routers, can contain valuable intellectual property and other sensitive information if not securely sanitised. Such items need to be securely destroyed to ensure confidentiality of any residual data.

5.1.1.5. Detection of abnormal and unauthorized sources of RF energy

- When the radar is being jammed there are several signal processing techniques that the Electronic Counter Counter Measures (ECCM) Radar Operator could use to counter the jamming. Some of these methods are normally installed in radars to overcome natural phenomena such as weather or ground clutter, but they are all considered ECCM.

5.2. Measures relating to access control

5.2.1. Fencing/Barriers

All ANS facilities and Ground Navaids and radar sites are all well protected with fencing and locked gate.

5.2.2. Entry Points Control

For all ANS staff and visitors, access to areas containing sensitive information must be physically restricted. This include but not limited to remote sites, control towers, technical rooms and training simulators. All individuals with access to these areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible. Individuals are also encouraged to challenge unescorted strangers and anyone not wearing visible identification. Access rights to secure areas are regularly reviewed and updated. A number of surveillance options are also available for provision of surveillance of the facility including human guards and screening machine at the main gates of ANS facilities. All CNS personnel will be required to wear office reflectors while operating in the airside areas. ANS Staff badges should have a specific period of validity, and the bearers should wear them visibly at all times in restricted areas.

5.2.3. Doors Opening Restriction

All doors accessing to ANS facility are locked with a Finger print access system. These facilities include control centers, control tower, NAVAIDS and radar sites, technical rooms and simulator training room.

5.2.4. Permit and Authorization

Procedures in respect of persons (such as visitors) and vehicles access

Detailed authorized access to a Restricted or Sterile Area at Kigali International Airport including ANS physical assets is controlled through the use of an Airport Restricted Area Permit (ARAP) system operated and controlled by RNP/ RDF that are found in the Airport Security Program (ASP) Section 3 Airport Security Measures. The purpose of this system is to identify persons and vehicles; and to facilitate access where authorized.

If allowed, visitors must be given a temporary facility badge allowing access to certain areas within the ANS facility and a log of this activity is retained for audit and security purposes.

5.2.5. Recruitment and Background Checks

The ANSP staff recruitment, background checks and personnel screening and vetting is conducted by proper authorities prior to selecting an individual for a position or authorizing an individual access as per the Airport Security Programme.

Detailed procedures are found in the Airport Security Program (ASP) chap 22 regarding SOP for the Recruitment of Staff Requiring Access to SRAs

5.2.6. In the Event of the main Power Failure

In the event that a power failure occurs in control, technical and simulator rooms, the following will be done:

a) Emergency lighting will be used to illuminate the working area before the main power is restablished;
b) Emergency lights are powered by rechargeable backup batteries which are either located inside the emergency light
c) UPS will be used to backup equipment in waiting the main power be restablished.

6. Airspace Management for ATM Security

ATM support on non-compliant aircraft

In situations, where the ATM/RAC is notified of a non-compliant aircraft by the State's defence or security organizations or where ATM/RAC identifies such aircraft by its own facility, the ATM/RAC shall locate and display the aircraft on the air traffic monitoring system.

In addition, the ATM/RAC shall assist in identifying and tracking the aircraft, and may be asked to provide to security partners the position, altitude, airspeed, and direction of flight.

The ATM/RAC also shall notify the affected ATC facility along the path of the track of interest and shall coordinate the tracking of the unknown aircraft until it lands.

Where any agreements/MoU may be in place with the Civil Aviation Authority, State military authorities and civil agencies, the ATM/RAC shall notify the designated authority when the aircraft lands.

In an emergency situation, the pilot-in-command, for the safety of the flight, may need to deviate from the rules. The ATM/RAC should take into consideration the safety of the flight and security requirements and advise the Pilot-in-Command to change the flight path accordingly.

Note: If an aircraft must be intercepted, Annex 2 — Rules of the Air

7. Security Response Plan

7.1. Risk Methodology

A risk assessment is a process which determines what information resources exist that require protection, and to understand and document potential risks from ANS security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. The risk assessment methodology forms part of a standard risk management process depicted below, which enables an organization to effectively identify, assess, and treat risk

The risk assessment methodology forms part of a standard risk management process depicted below, which enables an organization to effectively identify, assess, and treat risk

A risk assessment is therefore performed to determine the most important potential security breaches to be addressed and evaluates these in terms of cost impact (consequence) and probability of occurrence (likelihood). Analyzing risk in this way can help determine appropriate security budgeting and policy. As part of this process, it is important to first establish the context for the risk assessment. Details steps and methods to be followed can be found in below figure.

7.2. Managing Cyber Risks

Air Navigation infrastructure management needs to be able to assess the impact of security and the lack of security on the net-centric aviation system performance. Suitable policies, procedures and processes need to be determined. Detection mechanisms need to be put in place to identify the presence of a threat and decision support tools are needed for threat evaluation and mitigation. An approach is needed that uses standardized mitigations and scopes each threat to a minimum risk manageable, based on established policies, rules, processes and procedures. The risks to ATM can be managed by first identifying the overall systems in a functional unit and the associated risks, e.g. LAN, computers, HVAC, WAN connection, radio systems, etc. For generic ATM systems, threats will exploit the vulnerabilities to create a risk, and the level of this risk will be unique to each ANSP and business unit, e.g. an IT system for business support

7.3. Risk assessment

ANSPs should conduct a risk assessment to determine the greatest risks to the organization and should consider assessing the adequacy of their cyber security controls against a recognized standard or framework.

This assessment can be scoped against a subset of controls or against a profile that matches an ANSP's operational environment and needs. The NIST Cybersecurity Framework is one of the standards available and provides a common taxonomy and mechanism, primarily focused towards organizations that provide critical national infrastructure, to:

1. Describe their current cyber security posture

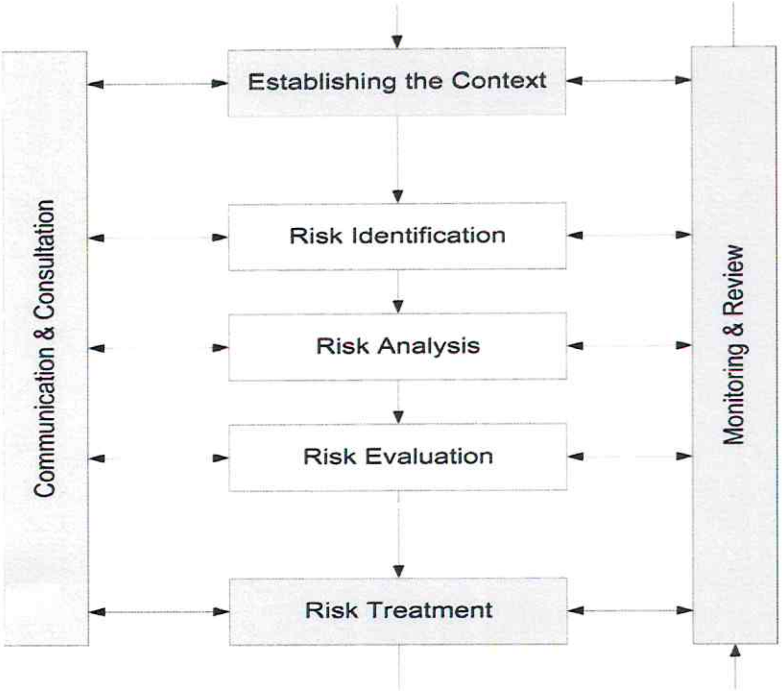
2. Describe their target state for cyber security

3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process

4. Assess progress toward the target state

5. Communicate among internal and external stakeholders about cyber security risk

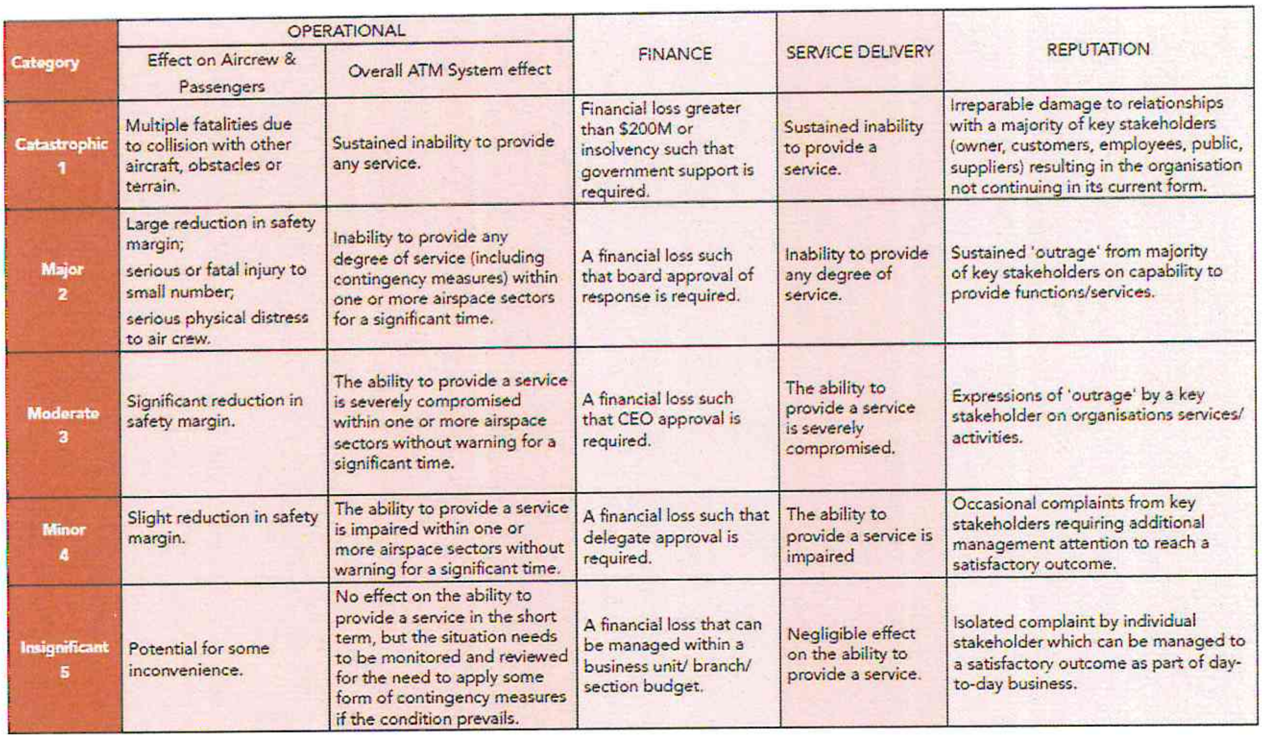
Figure 1: Risk management process



Because economics, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. Objectives must be established before administrators can identify and take necessary steps to manage risks. ANS Safety Manager, with the aid of ANS safety committees and other departments, will conduct a regular at least once every three months risk assessment in order to:

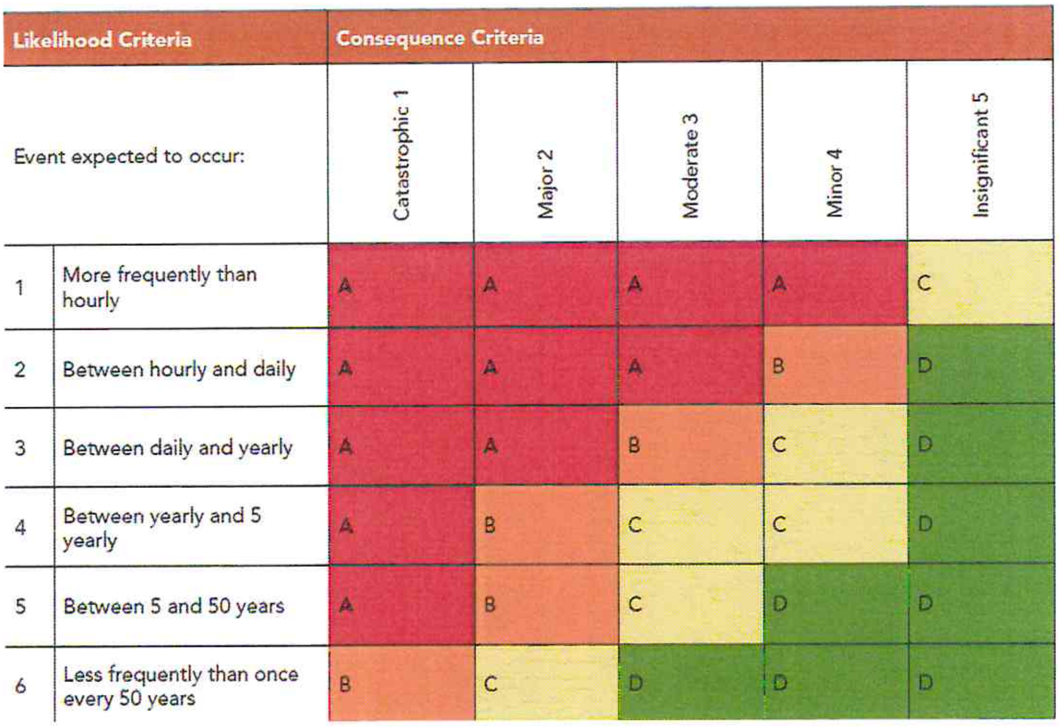
- Inventory and determine the nature of ANS information resources
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources
- Identify the level of security necessary for the protection of the ANS facilities.

If gaps are discovered, recommendations will be made to the Managing Director mitigate potential risk.



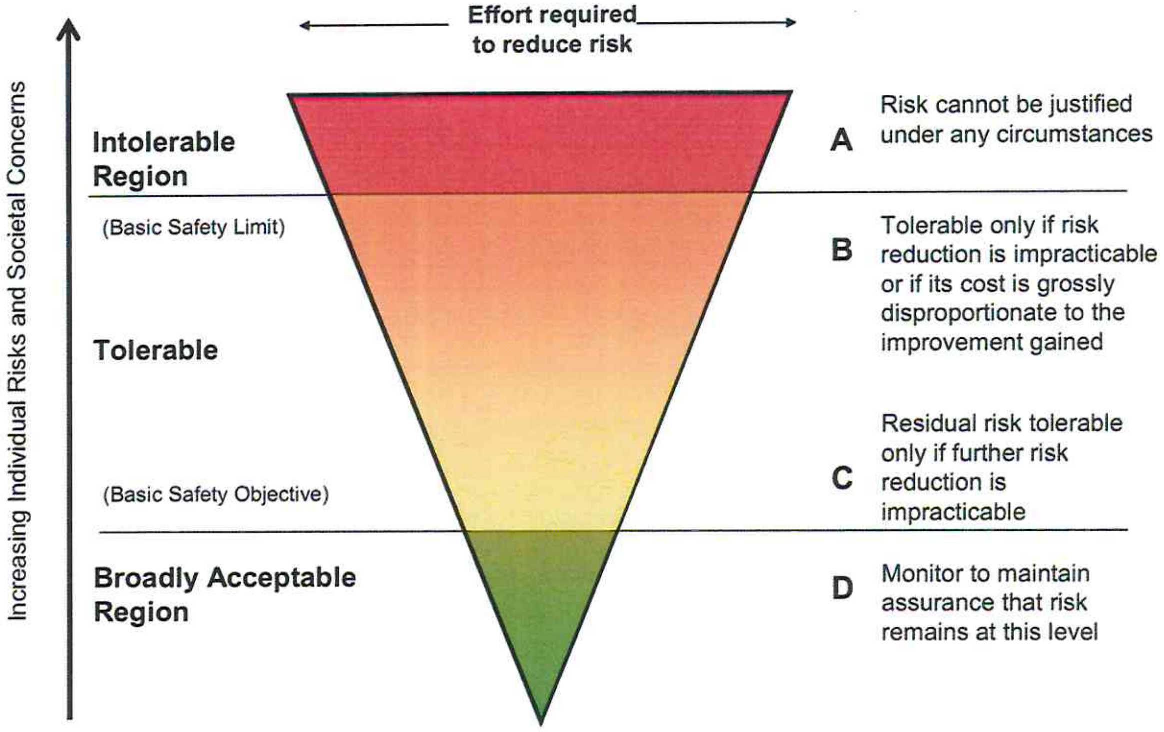
Category	OPERATIONAL		FINANCE	SERVICE DELIVERY	REPUTATION
	Effect on Aircrew & Passengers	Overall ATM System effect			
Catastrophic 1	Multiple fatalities due to collision with other aircraft, obstacles or terrain.	Sustained inability to provide any service.	Financial loss greater than $200M or insolvency such that government support is required.	Sustained inability to provide a service.	Irreparable damage to relationships with a majority of key stakeholders (owner, customers, employees, public, suppliers) resulting in the organisation not continuing in its current form.
Major 2	Large reduction in safety margin; serious or fatal injury to small number; serious physical distress to air crew.	Inability to provide any degree of service (including contingency measures) within one or more airspace sectors for a significant time.	A financial loss such that board approval of response is required.	Inability to provide any degree of service.	Sustained 'outrage' from majority of key stakeholders on capability to provide functions/services.
Moderate 3	Significant reduction in safety margin.	The ability to provide a service is severely compromised within one or more airspace sectors without warning for a significant time.	A financial loss such that CEO approval is required.	The ability to provide a service is severely compromised.	Expressions of 'outrage' by a key stakeholder on organisations services/ activities.
Minor 4	Slight reduction in safety margin.	The ability to provide a service is impaired within one or more airspace sectors without warning for a significant time.	A financial loss such that delegate approval is required.	The ability to provide a service is impaired	Occasional complaints from key stakeholders requiring additional management attention to reach a satisfactory outcome.
Insignificant 5	Potential for some inconvenience.	No effect on the ability to provide a service in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency measures if the condition prevails.	A financial loss that can be managed within a business unit/ branch/ section budget.	Negligible effect on the ability to provide a service.	Isolated complaint by individual stakeholder which can be managed to a satisfactory outcome as part of day-to-day business.

Assessment of the level of risk and risk tolerance



Likelihood Criteria		Consequence Criteria				
Event expected to occur:		Catastrophic 1	Major 2	Moderate 3	Minor 4	Insignificant 5
1	More frequently than hourly	A	A	A	A	C
2	Between hourly and daily	A	A	A	B	D
3	Between daily and yearly	A	A	B	C	D
4	Between yearly and 5 yearly	A	B	C	C	D
5	Between 5 and 50 years	A	B	C	D	D
6	Less frequently than once every 50 years	B	C	D	D	D

We have reviewed all identified risks and provided for each an overall risk ranking which is a combination of the two characteristics of consequence and likelihood. For example, a risk with a major consequence but a "5" likelihood would be described as having a "B" or "tolerable" risk rating. The previous matrix provides a guide to determine which risks are the highest priorities from the perspective of the timeliness of the corrective action required. The following diagram outlines the position in more definitive terms.


Effort required to reduce risk
Increasing Individual Risks and Societal Concerns
Intolerable Region
(Basic Safety Limit)
Tolerable
(Basic Safety Objective)
Broadly Acceptable Region
A
Risk cannot be justified under any circumstances
B
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
C
Residual risk tolerable only if further risk reduction is impracticable
D
Monitor to maintain assurance that risk remains at this level

7.4. Perform Control Activities

Following internal controls, procedures, and practices are to be regularly done by the ANS Safety Manager through internal audit:

- Risks are identified and reduced to an acceptable level

- All assets are safeguarded against waste, fraud, loss, unauthorized use or disclosure, and misappropriation

- Programs are efficiently and effectively carried out in accordance with applicable laws and security regulation. ANS relies on internal controls to remain in compliance with internal and external requirements.

7.5. Backup and Recovery

All ANS aeronautical and traffic data information is to be copied onto secure storage media on a daily basis (i.e., backed up), for the purpose of disaster recovery and investigation purpose. *The Backup and Recovery procedures in the CNS MANSOP*

"CHAP 7: Maintenance of documents and records" outlines the minimum requirements for the recorders, Impounding of Tapes and CDs, and disposal of Records

All backups conform to the following best practice procedures:

- All data and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates)

- Records of what is backed up and to where must be maintained

- Records of software licensing should be backed up

- The backup media must be precisely labeled and must have, at a minimum, the following identifying markers that can be readily displayed by labels and/or a barcoding system

7.6. Emergency Security Control of Air Traffic Priority

7.6.1. Emergency Coordination Procedures

The procedures outlined herein are intended as a general guide to air traffic services personnel for complete coordination with pilot in command when handling emergency situations.

In the event of an aircraft in, or appearing to be in, any form of emergency, every assistance shall be provided by the controller, and the procedures prescribed herein may be varied according to the situation:

i) The progress of an aircraft in emergency shall be monitored and (whenever possible) plotted on the situation display until the aircraft passes out of coverage of the ATS surveillance system, and position information shall be provided to all air traffic services units which may be able to give assistance to the aircraft. Transfer to adjacent sectors shall also be effected when appropriate.

ii) Whenever a ATS surveillance system emergency alert is observed on the situation display and there is no other indication of the particular nature of the emergency, the controller shall take the following action:

a) attempt to establish communication with the aircraft to verify the nature of the emergency; or

b) if no response is received from the aircraft, the controller shall attempt to ascertain if the aircraft is able to receive transmissions from the air traffic control unit by requesting it to execute a specified manoeuvre which can be observed on the situation display.

When an emergency is declared by an aircraft, the ATS unit should take appropriate and relevant action as follows:

a) unless clearly stated by the flight crew or otherwise known, take all necessary steps to ascertain aircraft identification and type, the type of emergency, the intentions of the flight crew as well as the position and level of the aircraft;

b) decide upon the most appropriate type of assistance which can be rendered;

c) enlist the aid of any other ATS unit or other services which may be able to provide assistance to the aircraft;

d) provide the flight crew with any information requested as well as any additional relevant information, such as details on suitable aerodromes, minimum safe altitudes, weather information;

e) obtain from the operator or the flight crew such of the following information as may be relevant: number of persons on board, amount of fuel remaining, possible presence of hazardous materials and the nature thereof; and

f) notify the appropriate ATS units and authorities as specified in local instructions.

Changes of radio frequency and SSR code should be avoided if possible and should normally be made only when or if an improved service can be provided to the aircraft concerned. Manoeuvring instructions to an aircraft experiencing engine failure should be limited to a minimum. When appropriate, other aircraft operating in the vicinity of the aircraft in emergency should be advised of the circumstances.

Note:- Requests to the flight crew for the information contained in 15.1.1.3 e) will be made only if the information is not available from the operator or from other sources and will be limited to essential information.

7.6.2. Unlawful interference and aircraft bomb threat

An aircraft known or believed to be in a state of emergency, including being subjected to unlawful interference, shall be given maximum consideration, assistance and priority over other aircraft as may be necessitated by the circumstances.

Air traffic services personnel shall be prepared to recognize any indication of the occurrence of unlawful interference with an aircraft.

Whenever unlawful interference with an aircraft is known or suspected or a bomb threat warning has been received, ATS units shall promptly attend to requests by, or to anticipated needs of, the aircraft, including requests for relevant information relating to air navigation facilities, procedures and services along the route of flight and at any aerodrome of intended landing, and shall take such action as is necessary to expedite the conduct of all phases of the flight, especially the safe landing of the aircraft.

ATS units shall also:

a) transmit, and continue to transmit, information pertinent to the safe conduct of the flight, without expecting a reply from the aircraft;

b) monitor and plot the progress of the flight with the means available, and coordinate transfer of control with adjacent ATS units without requiring transmissions or other responses from the aircraft, unless communication with the aircraft remains normal;

c) inform, and continue to keep informed, appropriate ATS units, including those in adjacent FIRs, which may be concerned with the progress of the flight;

Note.— In applying this provision, account must be taken of all the factors which may affect the progress of the flight, including fuel endurance and the possibility of sudden changes in route and destination. The objective is to provide, as far in advance as is practicable in the circumstances, each ATS unit with appropriate information as to the expected or possible penetration of the aircraft into its area of responsibility.

d) notify:

1) the operator or its designated representative;

2) the appropriate rescue coordination centre in accordance with appropriate alerting procedures;

3) appropriate authority designated by the state;

e) relay appropriate messages, relating to the circumstances associated with the unlawful interference, between the aircraft and designated authorities.

7.6.3. Bomb or other explosive device:

The following additional procedures shall apply if a threat is received indicating that a bomb or other explosive device has been placed on board a known aircraft.

The ATS unit receiving the threat information shall:

a) if in direct communication with the aircraft, advise the flight crew without delay of the threat and the circumstances surrounding the threat; or

b) if not in direct communication with the aircraft, advise the flight crew by the most expeditious means through other ATS units or other channels.

7.6.4. Emergency descent

Upon receipt of advice that an aircraft is making an emergency descent through other traffic, all possible action shall be taken immediately to safeguard all aircraft concerned. When deemed necessary, air traffic control units shall immediately broadcast by means of the appropriate radio aids, or if not possible, request the appropriate communications stations immediately to broadcast an emergency message.

Phraseology: ATTENTION ALL AIRCRAFT IN THE VICINITY OF (or AT) (significant point or location) EMERGENCY DESCENT IN PROGRESS FROM (level) (followed as necessary by specific instructions, clearance, traffic information etc.)

7.6.5. Testing procedures.

To insure that implementing actions can be taken expeditiously, tests will be conducted periodically twice a year in accordance with MATS under supervision of the Chief Air Traffic Management.

7.7. Physical access authorization

7.7.1. Authority and Responsibilities

Airport Operation Unit in charge of operations is responsible for the control of access to airside and into the SRA. This empowers the Airport Operation Unit and the relevant Authorities to deny access to any person who fails to comply with access control requirements.

7.7.2. Control of access – persons

Persons are only allowed to access Airside and the SRA through a security controlled access post or through a facility that is subject to a written access control approval.

Holders of permanent Airport security permits are permitted unescorted access to the Airside and SRA. Holders of visitor security permits must be escorted at all times when within the Airside and SRA.

Access controls can be both physical and logical, i.e. barriers that require a proximity card to gain access to the building are physical controls whereas digital access rights linked to a user account managed through Active Directory are logical controls. Refer to Chapter……below page 21 for details.

7.7.3. Control of access – vehicles

Vehicles are only allowed to access Airside and the SRA through a security controlled access post as long as they have been authorized.

7.7.4. Control of access – exemptions

Only those persons and vehicles provided with permanent access badges that allows them to access airside and SRA areas are exempt access control requirements.

7.7.5. Personnel screening and vetting

The Air Navigation Services ensures that background screening is conducted by proper authorities prior to selecting an individual for a position or authorizing an individual access to the ICT system. The Air Navigation Services accepts the eligibility of an individual from another organization that has conducted a comparable background screening, if it is approved by national laws or regulations. The Air Navigation Services shall also establish or follow prescribed conditions and frequencies for rescreening. Different rescreening conditions and frequencies may be required for personnel accessing the ICT system, based on the sensitivity of the position and information processed, stored or transmitted by the system. In addition, the Air Navigation Services shall ensure that all persons together with items carried are subject to screening and security controls prior to entry into facility security restricted areas serving civil aviation operations.

7.7.6. Personnel termination

Upon termination of an individual's employment, the Air Navigation Services:

(a) Terminates his/her access to restricted facilities and ICT systems;
(b) Conduct exit interviews;
(c) Retrieve all security-related organizational property, including ICT systems; and

(d) Retain access to organizational information and ICT systems formerly controlled by the terminated individual.

Exit interviews ensure that individuals understand the security constraints imposed by being a former employee, and that proper accountability is achieved. Examples of security-related property are authentication tokens, system administration technical manuals, keys, identification cards, and building passes.

7.7.7. Personnel transfer

The Air Navigation Services shall review physical and logical access authorizations to facilities, information, and ICT Systems when personnel are reassigned or transferred to other positions within RAC, whether it is temporary or permanent. The Air Navigation Services shall initiate these organization-defined transfer or reassignment security actions within a specified time, following the formal transfer action.

Examples of actions that may be required include:

(1) Returning old and issuing new keys, identification cards, and building passes;

(2) Closing previous ICT system accounts and establishing new accounts;

(3) Changing ICT system access authorizations; and

(4) Providing for access to official records which the employee had access to at the previous work location and in the previous ICT system accounts.

7.7.8. Access agreements

The Air Navigation Services identifies situations where an access agreement is required, prior to granting access to information and ICT systems. Information requiring special protection measures includes privacy information and proprietary information. In order to access certain security sensitive information Air Navigation services requires agreement with individuals assigned to access such information.

Examples of access agreements include nondisclosure agreements, acceptable-use agreements, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the ICT system to which access is authorized.

7.8. Navigational and other Vital Facilities

7.8.1. Authority and responsibilities

Responsibilities for the protection of vital facilities inside/outside of the Airside area and SRA are as follows:

Facility	Responsible Organization
Air traffic control rooms and equipment	Authorization required
Radar Sites	Escort required
ILS sites	Escort required
DVOR/DME	Escort required
AWOS	Escort required
VSAT Communication	Escort required

7.8.2. Protection of facilities

Air Navigation Services is responsible for determining the level of protection and monitoring required at its facilities and for detailing this in its Security Programme.

Air Navigation Services represented by a senior Air Traffic controller attends the Airport Security Committee (ASC) meeting where the risks to aviation and the protection of facilities are discussed.

7.8.3. Control of access to facilities

Air Navigation Services is responsible for determining the appropriate access control measures required at its facilities.

8. Evaluation and Auditing

Air Navigation Services need to implement and maintain quality controls in its departments security programme to determine compliance with and to validate the effectiveness of the programme.

Audits, tests, survey and inspections should be carried out on a regular basis to verify compliance with regulatory requirements and performance objectives set in the security programme as follows:

Internal Evaluations: All concerned ANS departments are encouraged to continuously and periodically monitor and evaluate these processes and procedures to determine their effectiveness and continuing applicability. Air Navigation Services Safety Manager will conduct quarterly an internal evaluation to assess whether the programme is working correctly and whether all aspects are still valid for current operations.

External audits of organizations will be conducted by national regulatory authorities as per the security regulations to obtain an objective view of the operator's security programme.

9. Air Traffic Management security incident reporting procedures

9.1. Air Traffic Incidents

The purpose of the reporting of aircraft incidents is to promote the safety and security of aircraft. The degree of risk involved in an aircraft incident should be determined in the incident investigation and classified as "risk of collision", "safety not assured", "no risk of collision" or "risk not determined".

An air traffic incident report shall be submitted, normally to the air traffic services unit concerned, for incidents specifically related to the provision of air traffic services involving such occurrences as aircraft proximity (AIRPROX), or other serious difficulty resulting in a hazard to aircraft, caused by, among others, faulty procedures, non-compliance with procedures, or failure of ground facilities.

Air Traffic Incident is used to mean a serious occurrence related to the provision of air traffic services, such as:

a) aircraft proximity (AIRPROX),

b) serious difficulty resulting in a hazard to aircraft caused, for example, by:

i) Faulty procedures,

ii) Non-compliance with procedures, or

iii) Failure of ground facilities.

The Air Traffic Incident Report Form (see Appendix I) is intended for use:

a) by a pilot for filing a report on an air traffic incident after arrival or for confirming a report made initially by radio during flight.

b) by an ATS unit for recording an Air Traffic Incident Report received by radio, telephone or teleprinter.

The purpose of the Air Traffic incident form is to provide investigatory authorities or enforcement organs with as complete information on an air traffic incident as possible and to enable them to report back, with the least possible delay to the pilot or operator concerned, the result of the investigation of the incident and, if appropriate, the remedial action taken.

Pilots will initially report an air traffic incident on radio to the relevant ATS unit and subsequently submit an air traffic incident report form (See Appendix I), upon arrival at destination, through the operator.

The ATS unit upon becoming aware of an air traffic incident will make an entry in the operational log book and subsequently fill the air traffic incident report form. The air traffic incident report form filled by an ATS unit should contain as much detail as is available to the ATS unit at the time of filling the report.

All air traffic incident report forms will be submitted to the head of ATM for investigation.

9.2. Air Traffic Services Messages

Air traffic services units may originate the following messages for transmission via the FIPS, aeronautical fixed telecommunication network (AFTN), direct-speech circuits as applicable. They are classified in categories relating to their use by the air traffic services. The priority indicator for AFTN is indicated in brackets. However with prior arrangement, the origination of these can be delegated to AIM, Communication or MET units as appropriate.

10. Security training

ANS staff need to be carefully selected and properly trained in security and supervised to ensure that they are consistently able to carry out their duties in a highly proficient manner.

Policy

Each employee, whether full-time, part-time or contract, should receive initial and recurrent security training commensurate with their duties. This is essential to alert employees to potential threats to the operator's facility and operations on an ongoing basis.

Training

Induction: Induction training for screening staff should comprise a combination of classroom and practical instruction utilizing equipment and techniques in use at the airport where the screeners will be employed. Induction training should be followed by a period of on-site training.

Refresher: refresher training at frequent intervals, every year should be provided. This training should be aimed at improving techniques, knowledge and motivation. Staff should be recertified in respect of their proficiency following refresher training.

Course Content:

At a minimum each employee will receive training in the following subjects:

- Aviation security overview
- Security awareness
- National security regulations

- ANS threat assessments/risk management
- ANS security programme
  - Policies
  - Organization/responsibilities
  - Facility physical security provisions/controls
  - Security procedures
- Relationship/coordination with security authorities/law enforcement personnel
- Personal identification
- Access controls
  - Facility
  - Personnel
  - Baggage/cargo
  - Vehicles
  - Aircraft
  - Surveillance
  - Reports
- Security response plan
  - Incident response/procedures

A detailed syllabus and lesson plan outline should be developed for the training programme. While the security coordinator is the logical choice for conducting the training courses, local security personnel may be used to provide more detail and lend credibility to the programme.

Each training session should be recorded in the employee's training record.

APPENDIX I

Air Traffic Incident Report Form

AIR TRAFFIC INCIDENT REPORT FORM

For use when submitting and receiving reports on air traffic incidents. In an initial report by radio, shaded items should be included.

A - AIRCRAFT IDENTIFICATION	**B - TYPE OF INCIDENT**
	AIRPROX/PROCEDURE/FACILITY*

C - THE INCIDENT

1. General

a) Date/Time of incident____________________________________UTC

b) Position

2. Own aircraft

a) Heading and route

b) True airspeed ____________________measured ( ) kt_______( ) km/h

c) Level and altimeter setting

d) Aircraft climbing or descending

( ) Level flight ( ) climbing ( ) Descending

e) Aircraft bank angle

( ) Wings level ( ) Slight bank ( ) Moderate bank

( ) Steep bank ( ) Inverted ( ) Unknown

f) Aircraft Direction of bank
( ) Left ( ) Right ( ) Unknown

g) Restriction to visibility (select as many as required

( ) Sun glare ( ) Windscreen pillar ( ) Dirty Windscreen

( ) Other cockpit structure ( ) None

* Delete as appropriate

h) Use of aircraft lighting 9 (select as many as required)

( ) Navigation lights ( ) Strobe lights ( ) Cabin lights

( ) Red anti –Collision lights ( ) Landing/taxi lights ( ) Logo (tail fin) lights

( ) Other ( ) None

i) Traffic avoidance advice issued by ATS

( ) Yes, based on ATS surveillance ( ) Yes, based on visual sighting ( ) Yes, based on other System information
( ) No

j) Traffic information issued

( ) Yes based on ATS surveillance ( ) Yes, based on visual sighting ( ) Yes, based on other system information

( ) No

k) Airborne collision avoidance system- ACAS

( ) Not carried ( ) Type ( ) Traffic advisory issued

( ) Resolution advisory issued ( ) Traffic advisory or resolution advisory not issued

l) Identification

( ) Not ATS surveillance system available ( ) Identification ( ) No identification

m) Other aircraft sighted

( ) Yes ( ) No ( ) Wrong aircraft sighted

n) Avoiding action taken

( ) Yes ( ) No

o) Type of flight plan IFR/VFR/none*

* Delete as appropriate

3. Other aircraft

a) Type and call sign/ registration 9 if known.

b) If a) above not known, describe below

( ) High wing (mid wing) ( ) Low

wing

( ) Rotorcraft

( ) 1 engine ( ) 2 engines ( ) 3 engines

( ) 4 engines ( ) More than engines

Marking, colour or other available details

____

c) Aircraft climbing or descending

( ) Level flight ( ) climbing ( ) Descending

( ) Unknown

d) Aircraft climbing or descending

( ) wings level ( ) slights bank ( ) moderate bank

( ) steep bank ( ) Inverted ( ) Unknown

e) Aircraft direction of bank

( ) left ( ) Right ( ) Unknown

f) Lights displayed

( ) Navigation lights ( ) Strobe lights ( ) Cabin lights

( ) Red anti-Collision lights ( ) Landing /Taxi lights ( ) Logo (tail fin) lights

( ) Other ( ) None ( ) Unknown

____

* Delete as appropriate

g) Traffic avoidance advice issued by ATS

( ) Yes, based on ATS Radar ( ) Yes, based on visual sighting ( )Yes, based on other information

( ) No ( ) Unknown

h) Traffic information Issued

( ) Yes, based on ATS Surveillance system ( ) Yes, based on visual sighting ( ) Yes, based on other information

( ) No ( ) unknown

i) Avoiding action taken

( ) Yes ( ) No ( ) Unknown

4. Distance

a) Closest horizontal distance ____________________________________

b) Closest vertical distance____________________________________

5.Flight meteorological conditions

a) IMC/VMC*
b) Above/bellow* clouds/fog/haze or between layers*
c) Distance vertically from cloud ___________ m/ft.* above
d) In cloud/rain/snow/sleet/fog/haze*
e) Flying into/out of* sun
f) Flight visibility ___________ m/km*

6. Any other information considered important by the pilot-in-command

____

____

____

____

* Delete as appropriate

D - MISCELLANEOUS

1. Information regarding reporting aircraft

a) Aircraft registration

b) Aircraft type

c) Operator

d) Aerodrome of departure

e) Aerodrome of first landing_______________________Destination

f) Reported by radio or other means to____________________(name of ATS unit) at date/time)_____________UTC

g) Date/time/place of completion of form

2. Function, address and signature of person submitting report

a) Function

b) Address

c) Signature

d) Telephone number

3. Function and signature of person receiving report

a) Function____________________________b) Signature

E - SUPPLEMENTARY INFORMATION BY ATS UNIT CONCERNED

1. Receipt of report

a) Report received via AFTN/radio/ telephone/ other (specify)*

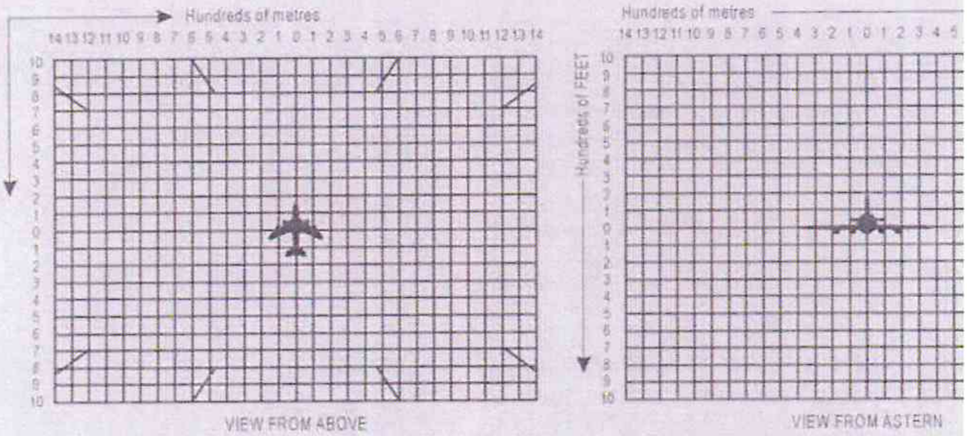
b) Report received by
(name of ATS Unit)

2. Details of ATS action

Clearance, incident seen (ATS surveillance system/visually, warming given, result of local enquiry, etc.)

DIAGRAMS OF AIRPROX

Mark passage of other aircraft relative to You, in plan on the left and in elevation on the right, assuming YOU are at the centre of each diagram. Include first sighting and passing distance.



Instructions for the Completion of the Air Traffic Incident Report Form

Item	
A	Aircraft identification of the aircraft filing the report
B	An AIRPROX report should be filed immediately by radio.
C1	Date / time UTC and position in bearing and distance from a navigation aid or in LAT/LONG
C2	Information regarding aircraft filing the report, tick as necessary
C2 c)	e. g. FL350 / 1013 hPa or 2500 FT / QNH 1007 hPa or 1200 FT / QFE 998 hPa.
C3	Information regarding the other aircraft involved.
C4	Passing distance - state units used.
C6	Attach additional papers as required. The diagrams may be used to show aircraft's positions.
D1 f)	State name of ATS unit and date time / time in UTC
D1 g)	Date and time in UTC.
E2	Include details of ATS unit such as service provided, radiotelephony frequency, SSR Codes assigned and altimeter setting. Use diagram to show the aircraft's position and attach additional papers as required.