Civil Aviation Authority of Singapore

Advisory Circular

AIRCRAFT NETWORK SECURITY PROGRAMME (ANSP)

GENERAL

Advisory Circulars (ACs) are issued by the Director-General of Civil Aviation (DGCA) from time to time to provide practical guidance or certainty in respect of the statutory requirements for aviation safety. ACs contain information about standards, practices and procedures acceptable to CAAS. An AC may be used, in accordance with section 3C of the Air Navigation Act (Cap. 6) (ANA), to demonstrate compliance with a statutory requirement. The revision number of the AC is indicated in parenthesis in the suffix of the AC number.

PURPOSE

This AC provides guidance to demonstrate compliance with, and information related to, requirements of the AOC holder on managing his aircraft network security programme as part of continuing airworthiness management of an aircraft.

APPLICABILITY

This AC is applicable to an AOC holder operating an aeroplane that has been specified by the aircraft manufacturer to require an ANSP. An aircraft requiring an ANSP to operate can be identified by a Special Condition (SC) listed on the Type Certificate Data Sheet (TCDS) or, if later modified, will be identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC) with a SC.

RELATED REGULATIONS

This Advisory Circular relates specifically to Regulation 129 of ANR-121.

RELATED ADVISORY CIRCULARS

Nil.

CANCELLATION
This AC supersedes AC AOC-37.

EFFECTIVE DATE
This AC is effective from 1 October 2018.

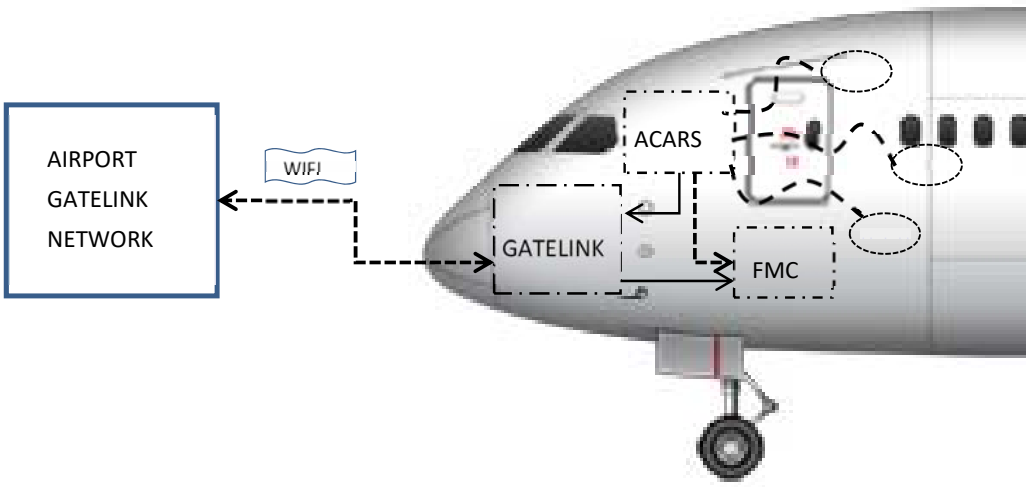
OTHER REFERENCES
- A350XWB Security Handbook
- 787 Airplane Network Security Operator Guidance (ANSOG)
- FAA AC 119-1
- CASA CAAP 232A-1

1 INTRODUCTION

1.1 Previously, aircraft used aviation (ARINC 429/ARINC 629) or military (MIL-STD-1553) standard data buses to connect flight avionics systems. Transmission Control Protocols (TCP) and/or Internet Protocols (IP) (TCP/IP) for passenger information and in-flight entertainment system were physically and logically isolated from the critical flight avionics system.

1.2 New aircraft designs utilize TCP/IP technology for the avionics systems (E-enabled aircraft), connecting both flight deck and cabin domains in a manner that virtually makes the aircraft an airborne interconnected network domain server. The architecture of this aircraft airborne network allows connectivity to external systems and networks, such as wireless airline operations and maintenance systems, satellite communications (SATCOM), email, the World Wide Web, etc. The major benefit of TCP/IP is the ability to move data to and from the aircraft without the use of standard storage media.

1.3 Ground servers (airport gatelink network) connected wirelessly to the aircraft network deliver software and also download data to/from the aircraft. This resulted in the introduction of new vulnerabilities that may open access to onboard aircraft systems and impede their operations, creating safety and airline business concerns.



1.4 During the software distribution from the suppliers/vendors, hackers can also attempt to manipulate and corrupt the critical software meant for updating aircraft avionics. The main safety threat is that intentional manipulation of genuine software or injection of fake software by well-informed hackers could go undetected.

1.5 Late detection of software manipulation, tampering with the aircraft administrative messages (i.e. upload commands, inventory requests and related responses) may lead, for instance, to false alarms, and general denial of services. Attacks on software distribution can all create unwarranted delays to flights and compromise safety.

1.6 In view of all of the above, the transmission of critical data necessitates the need for an Aircraft Network Security Programme (ANSP) by the AOC holder to ensure proper control during software handling/distribution and network security onboard the aircraft.

1.7 The ANSP starts from the point whereby the software vendor/supplier transmits the software electronically (via internet) to the AOC holder and from the AOC holder

through the wireless network or maintenance laptop to the aircraft. Thereafter, an approved person on the aircraft loads the software to execute the programme. Any changes made to the software configuration on the aircraft are treated with the same airworthiness intent as physical parts and will require the issue of a Certificate of Release to Service.

2 THREATS TO AIRCRAFT NETWORK SECURITY ARCHITECTURE

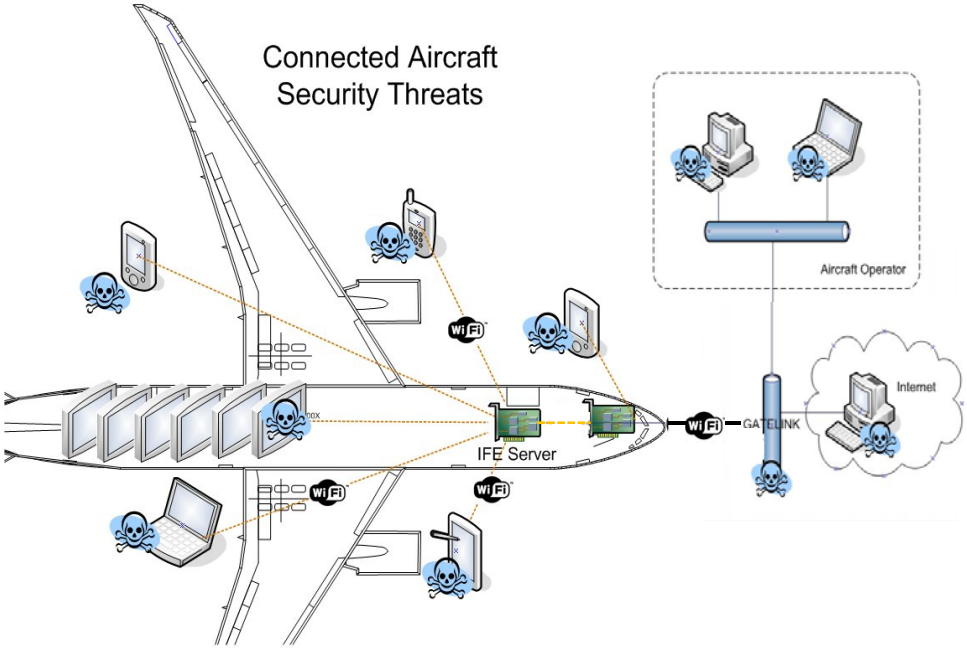
2.1 Onboard wired and wireless devices may have access to the aircraft network system to re-programme flight critical avionics components and may result in cyber security vulnerabilities from intentional or unintentional corruption of data and/or systems critical to the safety and continued airworthiness of the aircraft.

2.2 Threats also exist at access points of transmission through internet between software vendor/supplier to its operator or its contractor and at points when the software is transmitted from the operator (airport gatelink) to the aircraft.

2.3 The ANSP should be designed to protect the usability, reliability, integrity, and safety of the network and data. Effective aircraft network security targets a variety of threats and stops them from entering or spreading on the aircraft network which are associated with airworthiness.

2.4 Network security threats today are spread over the Internet. The most common include:

- Viruses, worms, and Trojan horses
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft



2.5 A successful attack can have an adverse effect on the aircraft and its occupants. Threats can cause a wide variety of failures.

General Threat Identifiers	Aircraft Data Network Threats	Example of operational impact
Failure	Safe state of the aircraft system could be compromised in the event of security penetration	Access to flight controls by unauthorised individuals affecting safety
Denial	Aircraft system resources exhausted due to denial of service attack, system error, malicious actions	Critical services disrupted by system overload or traffic jamming
Access Control	Individual other than an authorised user may gain access to the aircraft system via an unauthorised controller, masquerade, spoofing system error or an attack for malicious purposes	Unauthorised Access
Passive Attack	Snooping or eavesdropping compromising security (misdirection). Flaws in security policies may lead to back door access	Unauthorised corruption or destruction of data causing unsafe flight conditions

Types of Failures

3 AIRCRAFT OPERATION THAT REQUIRES ANSP

3.1 Aircraft with TCP/IP network systems are certificated through various means, such as Type Certificates (TC) and Supplemental Type Certificates (STC) that include Special Condition requirements (as with Boeing aircraft), or the Airworthiness Limitation Section (ALS) of the instructions for continued airworthiness (as with Airbus).

3.2 The FAA requires that the Type Design Holder issue a Network Security Document to provide the AOC holder with the information necessary to maintain his aircraft in compliance with the Special Conditions. This document would then be used by the AOC holder as the basis to construct his ANSP Document. Similarly, EASA requires its Type Design Holder to issue a Security Document to provide the AOC holder with information to construct his ANSP Document. Whenever there is a revision to the Security Document, the AOC holder's ANSP Document should also be revised as soon as possible.

3.3 The aircraft Type Certificate holder (e.g. Boeing/Airbus) will also provide instructions on how to maintain the aircraft onboard network system to ensure system integrity and security. These instructions can be found in the Aircraft Maintenance Manual, Fault Isolation Manual, Service Letters or Service Bulletins.

3.4 The AOC holder is reminded to follow instructions regarding aircraft network security as specified in the documentations issued by the Type Certificate holder and also the actions recommended in this AC.

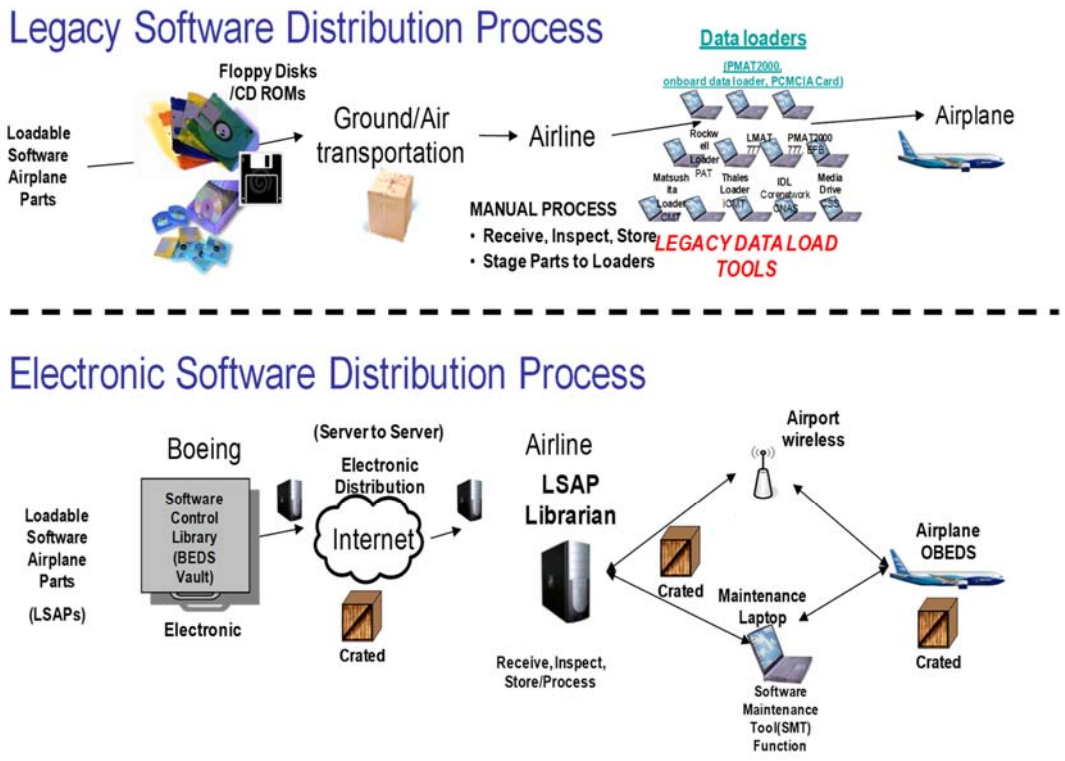
4 SOFTWARE DISTRIBUTION AND STORAGE

4.1 The aircraft uses software to provide logic or control for various system operations and functions and are regularly updated. The software is commonly known as Loadable Software Aircraft Part (LSAP) and is considered as part of the aircraft's configuration. The LSAPs for the aircraft are constantly being reviewed and upgraded by the aircraft avionics OEMs. Once new or upgraded version software are certified, it can be distributed to AOC holders for uploading onto the aircraft Onboard Electronic Distribution System (OBEDS).

4.2 Physical media such as CDs and DVDs have been used for managing, handling and distributing of LSAP. The distribution of LSAP may be over an online delivery medium such as the internet, without the use of physical media and then validated at the receiver's end. This is referred to as the Electronic Distribution of Software (EDS). As mentioned, threats exist at access points of transmission and therefore, require some form of mitigation.

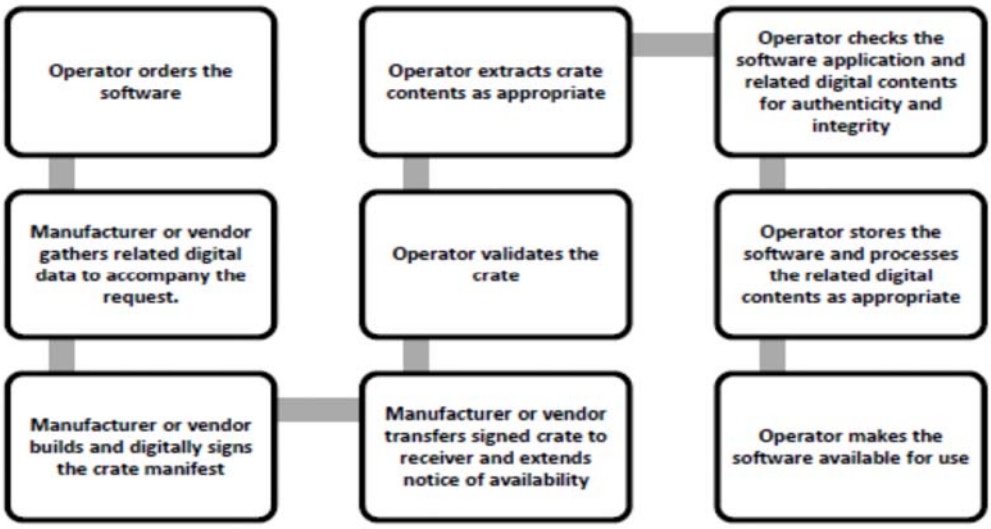
4.3 Process validation of Electronic Distribution of Software (EDS) crates with the authorised manufacturers is important. The AOC holder should verify the authenticity of the software. Aircraft configuration and software used for this purpose will require protection from data corruption, which includes damage caused by unauthorised users, viruses or other malware. The AOC holder should follow instructions from authorised manufacturer and crates that are unable to be identified and verified should be destroyed.

4.4 The diagram below shows the distribution of software from the vendor/supplier to the operator storage facility using physical media and EDS Process through the internet. The crated software can be loaded onto the aircraft wirelessly or via a maintenance laptop.



Electronic Distribution of Software

4.5 The following example of software distribution is typical of the process used to prepare and send software applications and other digital content.



Digital Distribution Process

5 AIRCRAFT MAINTENANCE

5.1 The AOC holder is ultimately responsible for the ANSP and should control every maintenance personnel (including contracted personnel) who may have access to or work on security sensitive systems.

5.2 The Maintenance Laptop is the primary maintenance system user interface with the aircraft that is used to update or change aircraft software configurations. Some Maintenance Laptops may make use of wireless connection to access aircraft software data. The access to and use of Maintenance Laptop should therefore be tightly controlled. Measures should be taken to make unauthorised use of wireless Maintenance Laptop difficult to accomplish and easy to detect. There should be an effective means of controlling access to onboard maintenance functions to prevent unauthorised access to aircraft systems and data. The AOC holder should also put in place a process to deal with the loss or corruption of these devices.

5.3 The AOC holder should also have a process for producing an authorised software configuration for his aircraft and also verifying his aircraft meets this configuration. Maintenance personnel should follow strictly the manuals/instructions from the aircraft manufacturer when implementing any changes to the aircraft configuration.

6 RISK ASSESSMENT.

6.1 Risk assessment is a fundamental component of risk management. The AOC holder should conduct risk assessments regularly to identify, estimate and prioritise risks to the aircraft network security programme. When weaknesses or deficiencies are discovered, mitigation measures should be imposed and changes to operator's policy should be made.

6.2 A security risk assessment is not complete until it includes the effects of all intended security controls and agreements with the involvement of any third parties.

6.3 The AOC holder should consider wider ranges of possible threat scenarios to determine the potential harms associated with the aircraft configuration and airworthiness. It is better to be over-inclusive with risks than under-inclusive when conducting this analysis. Changes to company policies may be required to mitigate particular risks by reducing the likelihood of occurrence.

6.4 The AOC holder should regularly reassess the ANSP to ensure that the security requirements continue to be valid. Changes in technology or to the AOC holder's business processes can possibly affect the validity of an ANSP. Any occurrences identified as threats should be reported to CAAS under Regulation 49 of ANR-91.

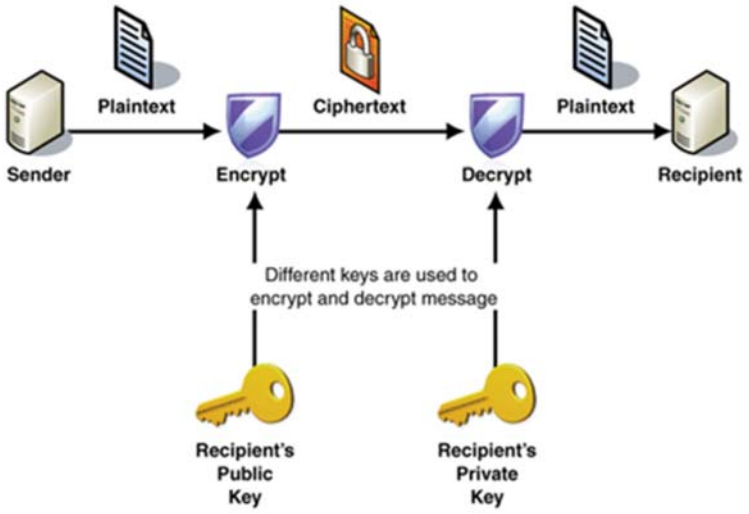
7 RISKS MITIGATION MEASURES

7.1 It is imperative that the AOC holder establishes good practices on aircraft software and network security in a manner similar to the IT security of an organisation. Failure to do so can compromise the airworthiness of the aircraft. Protection on wireless nodes should involve user authentication and data encryption. The encryption process transforms intelligible data, called plaintext, into an unintelligible form, called cipher text through the use of key.

Encryption/Decryption process

7.2 Decryption reverses this process, back to plaintext. If the cipher text changes in any way, it will not be decrypted correctly. Cryptography can therefore detect both intentional and unintentional modification.

7.3 A common technique employed is known as Public Key Infrastructure (PKI). In order to decrypt a file, a key pair is required. The public key is widely distributed, while only the recipient has access to the private key. The public key enables users to verify signatures while the private key allows for decryption of an encrypted file. Security of the private key is important to keep the plaintext secret.



Public Key Encryption

7.4 A digital signature is used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document sent is unchanged.

7.5 Mitigating measures should be documented for assurance purposes. The AOC holder should classify and treat documentation on mitigating measures as confidential documents.

7.6 Any wireless service providers used for the transfer of data should be evaluated for security risks. They should be documented in policies and procedures.

7.7 As far as mitigation measures are concerned, Point-to-Point connection is strongly preferred when performing software loading.

8 SECURITY LOGS

8.1 The AOC holder should establish a log of authorised users who have access to change or amend the aircraft software configuration. The AOC holder can monitor the ANSP with security logs. Computer security logs are audit logs that track any user authentication attempts. Security device logs are utilised to record any possible hardware attacks. Log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period.

8.2 An attack of the system may have taken place when the log shows any of the following:

- Unusually heavy network traffic;
- Out of disk space or significantly reduced free disk space;
- Unusually high CPU usage;
- Creation of new user accounts;
- Attempted or actual use of administrator-level accounts;
- Locked-out accounts;
- Account in-use when an authorised user is not at work;
- Cleared log files;
- Full log files with unusually large number of events;
- Antivirus or other alerts;

- Disabled antivirus software and other security controls;
- Unexpected update changes;
- Machines connecting to outside IP addresses;
- Requests for information about the system (social engineering attempts);
- Unexpected changes in configuration settings; and
- Unexpected system shutdowns.

9 AIRCRAFT SECURITY LOGS

9.1 An aircraft security log should be maintained for each aircraft. The AOC holder should specify in his ANSP the frequency, methods of storage, retrieval and analyses of aircraft security logs. The aircraft security log is to be analysed for anomalies to understand normal system behaviour and identify security risks. It is beneficial to create duplicate log files, one file for immediate analysis and one for unaltered history.

9.2 Automated downloading of the aircraft security log files is not considered a maintenance task unless specified by the aircraft manufacturer.

10 PASSWORD CONTROL

10.1 Password control is considered the simplest and most common form of user authentication. Password vulnerabilities can be reduced by changing passwords periodically and by using an active password checker that prohibits weak, recently used, or commonly used passwords.

10.2 The AOC holder should keep private and public keys as secure as possible. A process for the loss of passwords should be addressed. In addition, a process is also required for expired or invalid digital signatures and certificates.

11 CRITICAL AREAS OF THE AIRCRAFT

11.1 The flight deck, aircraft Electrical & Electronic Bays are critical areas of aircraft whereby equipment such as the wired Maintenance Laptop and automated test equipment interfaces with the aircraft avionics are located. These areas should be restricted to authorised personnel only.

11.2 The AOC holder should ensure that unauthorised physical access to Cabin Attendant Stations/Panels is prevented, particularly when passengers are moving about the cabin.

12 AIRCRAFT NETWORK ADMINISTRATOR.

12.1 The AOC holder should appoint an administrator to be responsible for the security of aircraft information network. The role of such an aircraft network administrator is similar in requirement to an IT network security manager.

12.2 The aircraft network administrator may be responsible to:

- Manage any lost or stolen Ground Support Equipment (GSE) devices that are required for changing aircraft software configuration.
- Create and control authorised user accounts.
- Decommission equipment or parts in a way that no data is recoverable from them.
- Provide logs, reports or other data to CAAS as required.
- Maintain a password management programme for users.
- Maintain records for equipment usage.
- Restrict any services, protocols, connections or nodes that are not required.
- Control access and utilisation for associated hardware required for aircraft network security programme.
- Quarantine any crates or files that contain invalid digital signatures, until there is a way of verifying the contents are authorised. Any invalidated crates should be deleted.
- Control of any cryptographic keys used in aircraft network security programme.
- Control of any aircraft network security programme certificate expiration dates.
- Identify and obtain aircraft software applications required for maintenance or modification of the aircraft configuration.
- Verify software applications and identify any issues with associated hardware used for their installation.
- Ensure suitable staging of software parts that will change aircraft configuration in a secure area, prior to installation on aircraft by appropriately licensed maintenance engineers.
- Retain and monitor aircraft network security programme logs.
- Retain any changes to the aircraft configuration
- Keep track of any changes required by the authorised manufacturer's software security processes.
- Update digital signatures if required for aircraft network security programme.
- Monitor any expiration of digital signatures.
- Eliminate any viruses or other malware that could affect the aircraft and/or systems required for the aircraft configuration.

13 TRAINING

13.1 Training for the aircraft network administrator should be provided so as to enable him to perform his role more effectively and efficiently. The scope of the training on the aircraft network security programme should be consistent with the requirements of the aircraft manufacturer.

13.2 Authorised personnel should be trained to understand good security practices and also be equipped with the ability to troubleshoot security related events. All personnel involved in ANSP should be familiar with the procedures defined in the ANSP.

14 USE OF CHECKLIST

The AOC holder should make use of appropriate checklists provided by the aircraft manufacturer in implementing a management process for his aircraft network security programme.