Civil Aviation Safety Authority
of Papua New Guinea

Advisory Circular

AC140-05

Aviation Security Risk Assessment Requirements

Initial Issue

07 May 2025

GENERAL

Civil Aviation Safety Authority of Papua New Guinea Advisory Circulars (AC) contain information about standards, practices and procedures that the Director has found to be an Acceptable Means of Compliance (AMC) with the associated rule.

An AMC is not intended to be the only means of compliance with a rule, and consideration will be given to other methods of compliance that may be presented to the Director. When new standards, practices or procedures are found to be acceptable, they will be added to the appropriate Advisory Circular.

PURPOSE

his Advisory Circular (AC) provides comprehensive technical and operational guidance for conducting aviation security risk assessments at civil aviation facilities in Papua New Guinea. It supports compliance with PNG Civil Aviation Rule (CAR) Part 140 and national security objectives

RELATED CAR

This AC relates to Rule 140.101 of PNG Civil Aviation Rules Part 140, which mandates operational performance testing and detection standards for all security screening equipment. It supplements Part 140, providing structured guidance for operators.

CHANGE NOTICE

This Advisory Circular (AC140-05) is the initial issue, introducing the first version of Aviation Security Risk Assessment Requirements.

TABLE OF CONTENTS

1. RISK ASSESSMENT STANDARDS AND METHODOLOGIES

1.1. Minimum Risk Assessment Criteria

Operators must conduct comprehensive risk assessments to identify potential security threats to civil aviation operations. The criteria should include:

(a) **Identification of potential threats and vulnerabilities** - Operators must systematically identify all potential threats and vulnerabilities that could impact aviation security. This includes assessing threats from various sources such as terrorism, insider threats, cyber-attacks, and other forms of unlawful interference.

(b) **Evaluation of the likelihood and impact** - Each identified threat must be evaluated in terms of its likelihood of occurrence and the potential impact on aviation operations. This involves qualitative and quantitative analysis to prioritize risks based on their severity and probability.

(c) **Development of mitigation strategies** - Based on the risk evaluation, operators must develop and implement effective mitigation strategies to address identified threats. These strategies should be tailored to reduce both the likelihood and impact of risks, ensuring a robust security posture.

(d) **Documentation and Reporting** - Operators must maintain detailed documentation of the risk assessment process, including methodologies used, findings, and mitigation measures. This documentation should be readily available for review by CASA PNG and other relevant authorities.

(e) **Regular Review and Update** - Risk assessments must be regularly reviewed and updated to reflect changes in the threat environment, operational conditions, and regulatory requirements. This ensures that risk management practices remain current and effective.

1.2. Risk Mitigation Strategies

Operators must implement effective risk mitigation strategies to reduce the likelihood and impact of identified threats. These strategies should be:

(a) **Aligned with National Security Objectives** - Mitigation strategies must support the overarching national security objectives and comply with relevant regulations and standards.

(b) **Based on Best Practices and Industry Standards** - Operators should adopt best practices and industry standards in developing and implementing mitigation measures. This includes leveraging guidance from ICAO Docs 8973 and 10047, as well as other relevant sources.

(c) **Integrated into Operational Procedures** - Mitigation strategies must be seamlessly integrated into the daily operational procedures of aviation security service providers. This ensures that risk management is an integral part of routine operations.

(d) **Subject to Continuous Improvement** - Operators should continuously monitor the effectiveness of mitigation strategies and make necessary adjustments to enhance security

measures. This involves regular performance testing, feedback collection, and iterative improvements.

2. TESTING METHODOLOGIES AND OPERATIONAL REQUIREMENTS

2.1 Performance Testing Requirements

Operators must conduct performance testing to verify the effectiveness of risk mitigation strategies. Testing should include:

(a) **Simulated Threat Scenarios** - Operators must design and execute simulated threat scenarios to test the robustness of mitigation measures. These scenarios should mimic real-world conditions and potential security threats.

(b) **Evaluation of Detection and Response Capabilities** - Performance testing should assess the ability of security systems and personnel to detect and respond to threats effectively. This includes evaluating detection sensitivity, response times, and overall system reliability.

(c) **Documentation of Testing Results and Corrective Actions** - Operators must document the results of performance testing, including any identified deficiencies and corrective actions taken. This documentation should be maintained for regulatory compliance and continuous improvement purposes.

2.2 Documentation and Compliance Reporting

Operators must maintain comprehensive documentation of risk assessments and performance testing. Compliance reporting should include:

(a) **Detailed Risk Assessment Reports** - Operators must produce detailed reports outlining the findings of risk assessments, including identified threats, risk evaluations, and mitigation strategies.

(b) **Performance Testing Results** - Documentation of performance testing results should include data on detection rates, false alarm rates, and overall system performance.

(c) **Records of Corrective Actions and Improvements** - Operators must keep records of any corrective actions taken to address deficiencies identified during risk assessments and performance testing. This includes documenting improvements made to security measures and systems.

3. TECHNICAL SPECIFICATIONS AND OPERATIONAL REQUIREMENTS

3.1 Certification and Standards

Operators must ensure that all security technologies and processes meet the certification and standards outlined in PNG CAR Part 140. This includes:

(a) **Certification of Security Equipment** - All security equipment used by operators must be accepted by the Director or other recognized authorities. Certification ensures that equipment meets the required performance and reliability standards.

(b) **Compliance with PNG CAR Part 140** - Operators must ensure that security technologies and processes comply with national standards, particularly those outlined in PNG CAR Part 140.

3.2 Procurement and Deployment

Operators must follow structured procedures for the procurement and deployment of security technologies. This includes:

(a) **Evaluation of Technology Specifications** - Operators must thoroughly evaluate the specifications of security technologies to ensure they meet operational requirements and regulatory standards.

(b) **Verification of Compliance with Regulatory Standards** - Before deployment, operators must verify that security technologies comply with all relevant regulatory standards and certifications.

(c) **Coordination with CASA PNG for Approval and Deployment** - Operators must coordinate with CASA PNG to obtain approval for the deployment of new security technologies. This includes submitting necessary documentation and undergoing required evaluations.

3.3 Maintenance and Calibration

Operators must develop and follow a manufacturer-approved preventive maintenance schedule. This includes:

(a) **Regular Calibration Checks** - Operators must conduct regular calibration checks to ensure the accuracy and reliability of security technologies.

(b) **Documentation of Maintenance Activities** - Operators must maintain detailed records of all maintenance activities, including calibration checks, software/firmware updates, and any identified faults or anomalies.

(c) **Ensuring Service Agreements with Qualified Technicians** - Operators must have service agreements in place with qualified technicians to perform maintenance and calibration activities.

3.4 Performance Testing

Operators must conduct regular performance testing to ensure the effectiveness of security technologies. This includes:

(a) **Testing Under Operational Conditions** - Performance testing must be conducted under real-world operational conditions to assess the effectiveness of security technologies.

(b) **Evaluation of Detection Capabilities** - Testing should evaluate the detection capabilities of security technologies, including sensitivity, accuracy, and reliability.

(c) **Documentation of Testing Results** - Operators must document the results of performance testing, including any identified deficiencies and corrective actions taken.

3.5 Training and Competency

Operators must ensure that personnel are trained in the operation, troubleshooting, and response protocols for security technologies. This includes:

(a) **Initial Training Prior to Operational Use** - Personnel must receive initial training before security technologies are put into operational use. This training should cover all aspects of operation, troubleshooting, and response protocols.

(b) **Annual Refresher Training** - Operators must provide annual refresher training to personnel to ensure they remain proficient in the use of security technologies.

(c) **Training Updates Following Significant Upgrades** - Operators must update training programs following significant upgrades to security technologies to ensure personnel are familiar with new features and functionalities.

3.6 Contingency Planning

Operators must develop contingency plans to address potential malfunctions or failures of security technologies. This includes:

(a) **Procedures for Equipment Calibration and Maintenance** - Contingency plans must include procedures for equipment calibration and maintenance to ensure continued reliability.

(b) **Alarm Resolution and Escalation Protocols** - Operators must establish protocols for resolving and escalating alarms to ensure timely and effective responses to potential security threats.

Appendix 1 – Sample Risk Assessment – XYZ Airport (No Perimeter Fencing)

This risk assessment examines the potential security vulnerabilities and operational risks associated with the absence of perimeter fencing around the boundary of XYZ Airport. It identifies and evaluates threats related to unauthorized access, wildlife intrusion, and other safety and security concerns that may arise due to the lack of a physical barrier. The assessment outlines the likelihood and consequences of these risks, and provides recommendations for mitigation measures to enhance the overall security posture of the aerodrome

Applicant:	XYZ Limited		
Aerodrome:	XYZ AIRPORT		
Designation:	Security Designated Aerodrome		
Security Concern:	No Security Perimeter Fencing		
Risk Assessment Title:	Assessment of Security Risks Due to Lack of Perimeter Fencing at XYZ Aerodrome	Version:	Initial
Type of Operation:	Domestic and International Operations		

1. THREAT IDENTIFICATION

This section identifies specific threats to the airport's operations. Each threat is evaluated based on its source, the likelihood of occurrence, its potential impact, and the overall risk level using a qualitative assessment approach.

Threat Description	Source	Likelihood	Impact	Risk Level
Unauthorized access to airside	Local intruders, opportunists	High	High	Critical
Sabotage of aircraft or infrastructure	Criminal or extremist actors	Low	High	High
Wildlife intrusion	Natural	High	Medium	High
Theft of aviation fuel or equipment	Opportunistic theft	Medium	Medium	Medium

2. VULNERABILITY ASSESSMENT

This section evaluates existing weaknesses in the current security setup that may increase the likelihood or impact of identified threats. These vulnerabilities are assessed to determine how exposed the airport is to the potential threats.

- No physical barrier to deter or delay unauthorized access.
- Limited surveillance coverage of perimeter areas.
- No patrols during night hours.
- No signage indicating restricted areas.

3. RISK EVALUATION

The overall risk is assessed by considering both the identified threats and the vulnerabilities. This evaluation uses qualitative matrix, allowing for an informed understanding of which risks are most critical and require immediate attention.

Using this approach, the absence of fencing results in multiple high to critical risk ratings, particularly for unauthorized access and wildlife intrusion.

4. MITIGATION MEASURES

This section outlines strategies to reduce the risks to acceptable levels. It includes specific mitigation actions, identifies responsible parties, and provides implementation timelines to address each risk.

Risk	Mitigation Strategy	Responsible Party	Timeline
Unauthorized access	Install temporary fencing and signage; deploy mobile patrols	Airport Operator	3 months
Wildlife intrusion	Clear vegetation and install wildlife deterrents	Airport Maintenance	1 month
Theft	Increase lighting and install CCTV at key access points	Airport Security	2 months

5. RESIDUAL RISK ASSESSMENT

After implementing the mitigation measures, this section reassesses the risk levels to determine whether they have been reduced to acceptable levels. This ensures that the airport is better protected and that any remaining risks are manageable.

Threat	Residual Risk Level
Unauthorized access	Medium
Wildlife intrusion	Low
Theft	Low

6. MONITORING AND REVIEW

This section outlines the ongoing processes that ensure continued effectiveness of the implemented mitigation measures. Regular reviews, updates, and audits help maintain an effective security posture over time.

- Monthly reviews of perimeter security effectiveness
- Quarterly updates to the risk register
- Surveillance audit by CASA PNG