Civil Aviation Safety Authority
of Papua New Guinea

Advisory Circular

AC100-7

Cyber Threat Management

Initial Issue

12 December 2025

GENERAL

Civil Aviation Authority 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

This Advisory Circular (AC) provides guidance to organisations required to comply with Civil Aviation Rule Part 100 on how to integrate cyber threat identification, risk management, mitigation, monitoring, training, and reporting into their Safety Management System (SMS) and Quality Management System (QMS).

RELATED CAR

This AC relates specifically to Civil Aviation Rules 100, 102, 109,119,137,139,140, 141, 144, 145, 146, 171, 172,173,174, 175 and 176 standards.

CHANGE NOTICE

There was no previous issue of this AC, consequently no change is in effect.

APPROVAL

This Advisory Circular has been approved for publication by the Director of Civil Aviation.

TABLE OF CONTENTS

CHAPTER 1 — INTRODUCTION

1.1 Introduction

1.1.1 The Papua New Guinea aviation system is increasingly dependent on interconnected information and communications technology (ICT). While these systems enhance efficiency and capability, they also introduce cyber threats that may affect aviation safety, continuity, and resilience.

1.1.2 This Advisory Circular provides guidance to aviation document holders on how cyber threats are to be identified, assessed, mitigated, monitored, and reported within the SMS and QMS frameworks mandated under CAR Part 100.

1.1.3 Cyber threats are treated as safety hazards where they have the potential to affect aviation operations, safety outcomes, or State Safety Programme (SSP) performance.

1.2 Definitions, Abbreviations and Units of Measure

1.2.1 Definitions

Cyber Threat	Any potential event or actor capable of compromising ICT systems, data, or aviation operations.
Cyber Hazard	A condition or vulnerability within ICT systems that may lead to unsafe aviation outcomes.
Unlawful Interference (Cyber)	Acts targeting aviation ICT systems to disrupt safety, security, or continuity

1.2.2 Abbreviations

AC	Advisory Circular
AMC	Acceptable Means of Compliance
CAR	Civil Aviation Rule
SMS	Safety Management System
QMS	Quality Management System
ICAO	International Civil Aviation Organization
ATS	Air Traffic Services
ALoSP	Acceptable Level of Safety Performance
ICT	Information and Communications Technology
ISCM	Information Security Continuous Monitoring
SIEM	Security Information and Event Management
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
SLAs	Service Level Agreements
SPIs	Safety Performance Indicators

1.2.3 Units of Measure

NIL

CHAPTER 2 — FORM, FUNCTION & FIT FOR CYBER THREAT MANAGEMENT

2.1 Form

Cyber threat management under CAR Part 100 is implemented through existing SMS and QMS structures. It does not require a standalone cybersecurity management system but must be demonstrably integrated into:

- Hazard identification processes
- Risk management processes
- Interface management
- Safety performance monitoring

2.2 Function

The function of cyber threat management is to:

- Prevent unsafe system states arising from cyber events
- Detect and respond to cyber-related hazards
- Support continuous improvement of safety performance
- Contribute State-level safety data and SSP outcomes

Organizations should establish a procedure to identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference by using the following criteria:

i) Identification & Classification

- Inventory of Critical Assets- identify and maintain an up-to-date inventory of ICT systems and data critical to aviation safety, security, and operations.
- Classification by Criticality- Classify assets based on operational impact (e.g., safety-critical, security-critical, facilitation-critical).

ii) Risk Assessment

- Holistic Threat Modeling -Conduct structured, risk-based threat assessments to identify potential threats and vulnerabilities.
- Risk Register-Maintain a centralized register of risks and associated mitigation measures.

iii) Protective Measures

- Administrative Controls
  - ✓ Policies, Procedures, and security awareness training
  - ✓ Defined roles, responsibilities, and segregation of duties
  - ✓ Personnel vetting and background checks
- Technical Controls
  - ✓ Firewalls, IDS/IPS, and endpoint protection
  - ✓ Network segmentation for safety and security domains
  - ✓ Data encryption (in transit and at rest)
  - ✓ Multi-factor authentication and strict access controls
- Physical Controls
  - ✓ Secure data centers and server rooms with limited access
  - ✓ Surveillance and intrusion detection systems
  - ✓ Access logs and physical entry controls

iv) Continuous Monitoring

- Implement Information Security Continuous Monitoring (ISCM)
- Use Security Information and Event Management (SIEM) systems
- Perform routine log analysis, vulnerability scans, and system audits

v) Incident Detection & Response

- Real-time monitoring and alerting of anomalies
- Clear incident response plan with severity classification
- Crisis communication plan and notification protocols
- Post-incident review and lessons learned

vi) Supply Chain Security

- Vet suppliers for cybersecurity practices
- Include security clauses in contracts and SLAs
- Monitor third-party compliance and system updates

vii) Training & Awareness

- Regular cybersecurity training for all aviation stakeholders
- Specialized training for ICT personnel and incident responders
- Simulation exercises (e.g., Tabletop Exercises)

viii) Post Event Analysis

Once an incident response has been concluded and aviation operations restored to a normal operating mode, conduction of a thorough analysis of the event is a critical step in ensuring that there is no future recurrence.

Analysis should be performed with third part system providers, manufacturers or appropriate authorities to help identify the root causes and identify cross-references to existing safety analyses/documentation.

All findings and final recommendations should be shared with states and the aviation industry stakeholders so that they may adjust their respective cybersecurity governance approach and programme.

2.3 Fitness

Cyber threat management must be proportionate to:

- The size and complexity of the organisation
- The criticality of ICT systems used
- The organisation’s role within the PNG aviation system

The approach must align with ICAO Annexes 17 and 19 and the State Safety Programme.

CHAPTER 3 — CYBER THREAT MANAGEMENT

3.1 Cyber Threat Management

Cyber threat management is the systematic application of policies, procedures, tools, and human factors to identify, control, and monitor cyber risks that may affect aviation safety. It follows the same safety logic as other hazards within SMS and is subject to the organisation's defined ALoSP.

3.2 Cyber Threats within SMS

Cyber threats must be included in:

- Hazard identification (Rule 100.59)
- Risk assessment and mitigation (Rule 100.61)
- Safety assurance and monitoring (Rule 100.77)

Examples include:

- System outages
- Data integrity compromise
- Ransomware affecting operational continuity
- Loss of surveillance, navigation, or communication capability

3.3 Cyber Threat Interfaces

Cyber risks frequently arise at interfaces with:

- External ICT providers
- Aerodrome systems
- ATS systems
- Data exchange partners

Organizations must define responsibilities and controls at these interfaces through formal agreements and oversight.

CHAPTER 4 — CYBER THREAT COMPLIANCE ELEMENTS

4.1 Acceptable Means of Compliance

Acceptable means of compliance include:

- Documented cyber hazard registers
- Risk assessments linked to operational impact
- Defined mitigations and monitoring mechanisms
- Training and awareness programmes
- Incident reporting and post-event analysis

Cyber-related safety actions must be traceable within SMS documentation and management review processes.

4.2 Rules of CAR Part 100

4.2.1 Rule 100.59(b)(3) – Inclusion of cyber threats in hazard identification

Part 100 requires organizations to include cyber threats as part of their hazard identification procedures. Organizations should:

(1) Identify cyber-related hazards affecting aviation operations, systems, personnel, and data.

(2) Include cyber incidents, attempted breaches, network degradation, and system manipulation as reportable hazards.
(3) Implement reporting channels that allow staff to report suspicious activity or cyber anomalies confidentially (Rule 100.67 & Rule 100.69).

4.2.2 Rule 100.61(b)(6) – Risk management of cyber threats, including human factors

Organizations must assess risks arising from cyber threats and apply mitigations accordingly. Risk management processes should include:

a. Cyber threat likelihood and severity evaluation
b. Application of mitigations consistent with industry cyber frameworks
c. Incorporation of human factor considerations (Rule 100.61(b)(5) when responding to cyber threats
d. Continuous monitoring of cybersecurity risk levels
e. Evidence-based follow-up to verify effectiveness of cyber mitigators (Rule 100.61(b)(4)

Cyber Risk Mitigation Measures:

- Multi-factor authentication
- Updated firewalls and intrusion detection systems
- Network segmentation of operational and administrative systems
- Regular software patching and updates
- Backup systems and disaster recovery plans
- Access control policies for operational environments
- Cybersecurity awareness programmes

4.2.3 Rule 100.63(b)(6) – Cyber threats at organizational interfaces

At all interfaces with external service providers, the organisation must identify and mitigate cyber threats. The organisation should:

a. Identify all external interfaces (IT service providers, fuel providers, airlines, cargo agents, third-party maintenance, data centres)
b. Define cyber responsibilities within Service Level Agreements (SLAs).
c. Ensure external providers comply with cyber safety requirements relevant to the operation.
d. Require periodic cybersecurity assurance statements or audit results.
e. Address cyber threats that may arise from data exchange across interfaces (Rule 100.63(b)(4).

4.2.4 Rule 100.71 – Cyber scenarios in emergency response planning

Cyber threat information must be communicated internally, with confidential reporting, just culture protections and reported to the Authority using Form CAA005. Organisations should:

a. Establish channels for reporting cyber incidents (Rule 100.69(b)(3)).
b. Ensure cyber reports are included in SMS performance reviews (Rule 100.77).
c. Communicate cyber trends, alerts, and mitigations to all operational personnel (Rule 100.67(a)).
d. Protect identities and ensure the use of just culture (Rule 100.69(b)(4)).

4.2.5 Rule 100.73 – Cybersecurity training requirements

Organisations must plan and conduct exercises that include cyber-related emergency scenarios. Emergency response plans should include:

- Cyberattack on aerodrome systems
- Outage of ATS/communication systems due to cyber intrusion
- Loss of critical navigation or surveillance data
- Ransomware attack affecting operational continuity
- Cyber crisis affecting multiple aviation partners

Training and simulation exercises must be conducted regularly as required by Rule 100.71(a)(4)

4.2.6 Rule 100.77 – Monitoring and measuring cyber-related safety performance

Cyber threat indicators must be monitored as part of safety performance. Possible Cyber Safety Performance Indicators (SPIs)

- Number of cyber incidents affecting operations
- Time to detect and respond to cyber events
- Number of cyber vulnerabilities identified and closed
- Percentage of staff completing cyber awareness training
- Number of cyber risks above ALoSP threshold
- Outputs should be routinely reported by Rule 100.77(c).

CHAPTER 5 — REFERENCES

1. Civil Aviation Rules – Part 100 (Amendment 3) — Cyber-related requirements introduced by Amendment 3 of Part 100, including Rules 100.59(b)(3), 100.61(b)(6), and 100.63(b)(6).
2. Civil Aviation Rules – Organizational Certificate Parts — Parts 102, 109, 119, 137, 139, 140, 141, 144, 145, 146, 171, 172, 173, 174, 175, 176 as prescribed under Rule Part 100.
3. ICAO Annex 17 (Amendment 18) Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference; cited for cybersecurity alignment.
4. ICAO Annex 19 (Amendment 2) -Safety Management; cited for integrating cybersecurity within SMS.
5. CAA005 - CASA PNG reporting form required for notifying the Authority of cyber threats/incidents.