AIRWORTHINESS NOTICE

No 43

Issue 1

November 2025

Implementation of Information Security Management (Part-IS) requirements to SCAA approved Part-CAMO and Part-145 organizations

1. Introduction

This notice aims to present the new EASA Regulation, 'Part-IS,' as it applies to Part-CAMO and Part-145 organizations under the Seychelles Civil Aviation Authority (SCAA) regulatory framework, focusing primarily on the associated Acceptable Means of Compliance (AMC's) and Guidance Material (GM's).

Information security is critical to aviation safety. This guidance is published to ensure that organizations and service providers manage information security consistently to protect aviation safety and enhance efficiency.

- **Information security** is defined as the protection of confidentiality, integrity, authenticity, and availability of network and information systems

- **Information security risk** is the risk to civil aviation operations, assets, individuals, and other organizations arising from potential information security incidents[5]. These risks stem from threats exploiting vulnerabilities in information assets or groups of assets

2. Regulation in Seychelles Context

The Civil Aviation (Safety) Regulations, 2017, regulation 110, empowers the Authority (SCAA) to issue civil aviation directives on matters prescribed by regulations.

The following Civil Aviation Directives establish the adoption of EASA requirements:

- **SCAA CAD-AIRW/10(Vc) - Approval for the Continuing Airworthiness Management Organisation**

- **SCAA CAD-AIRW/11 - Maintenance Organisation Approval**

These directives state that the requirements for Continuing Airworthiness Management Organisations and Maintenance Organisations are those laid down in **EASA Part-CAMO** and **EASA Part-145** (respectively), inclusive of all associated AMC's and GM's, as defined by EASA.

Regulation 111 of the Civil Aviation (Safety) Regulations, 2017, mandates that amendments to the adopted standards become effective unless the contrary is expressly stated in the Civil Aviation directive.

The new requirements are introduced by **EASA Regulation (EU) No 2023/203**, which is set to apply on **22 February 2026**. Annex VII of this regulation introduces amendments regarding the requirements for the management of information security risks with a potential impact on aviation safety.

In the airworthiness perspective, these amendments apply to:

- Maintenance organisations subject to Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014, **except** those solely involved in the maintenance of aircraft in accordance with Annex Vb (Part-ML)
- Continuing airworthiness management organisations (CAMOs) subject to Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014, **except** those solely involved in the continuing airworthiness management of aircraft in accordance with Annex Vb (Part-ML)

The amendment introduces new headings to Part-CAMO and Part-145.

Part-145 (Maintenance Organisations)	**Part-CAMO (Continuing Airworthiness Management Organisations)**
145.A.200A - Information security management system	CAMO.A.200A - Information security management system
145.B.135A - Immediate reaction to an information security incident or vulnerability with an impact on aviation safety	CAMO.B.135A - Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

3. Information Security Management System (ISMS)

The Information Security Management System (ISMS) is modeled after the Safety Management System (SMS), allowing the foundational pillars of SMS to be effectively applied within the ISMS framework.

Key requirements for organizations (in principle) include:

- Establish an information security policy, defining its scope and objectives;
- Appoint competent personnel to manage information security (IS);
- Define criteria for evaluating the trustworthiness of IS personnel;
- Implement measures to detect, respond to, and recover from security incidents;
- Establish internal and external reporting mechanisms for security matters;
- Identify and manage information security risks;
- Monitor and assess key performance indicators (KPIs) regularly;
- Implement compliance monitoring to ensure the effective operation of the ISMS;
- Provide training and raise awareness among personnel regarding information security.

CAMO and AMO organizations shall establish ISMS in **Present** and **Suitable** maturity levels at the time of the entry into force of the Part-IS requirements.

The SCAA Airworthiness Inspectorate will monitor the implementation and maturity of the ISMS using the SCAA Information Security Compliance Checklist (SCAA Form SF 58) and SCAA Part-IS audit checklist.

Definition used in the tool – maturity levels	
Present	There is evidence that the relevant item is documented within the organisation's Management System Documentation.
Suitable	The relevant item is suitable based on the size, nature, complexity of the organisation and the inherent risk in the activity.

4. Information Security Management Manual (ISMM)

The Information Security Management Manual (ISMM) can be a standalone document or integrated within the Safety Management Manual (SMM/MSM) of the operator, provided it includes all elements listed in IS.I.OR.250(a)

The ISMM must include:

- A statement signed by the Accountable Manager confirming compliance with the Annex and the ISMM, countersigned by the Chief Executive Officer (CEO) if the Accountable Manager is not the CEO;
- The organization's information security policy;
- The title(s), name(s), duties, accountabilities, responsibilities, and authorities of appointed information security personnel;
- An organizational chart;
- The internal reporting scheme;
- Procedures detailing how the organization ensures compliance with the Part, including documentation, management of contracted activities, and the ISMM amendment procedure;
- The organization's data retention policy.

5. Personnel and Personnel Competence

The Accountable Manager (AM) shall appoint a person or group of persons responsible for ensuring compliance with Part-IS. This responsibility may be delegated to a **Common Responsible Person** (CRP), such as a Chief Information Security Officer

Appointed personnel must possess the necessary **competence** and demonstrate **trustworthiness**. The criteria for evaluating these shall be clearly defined, implemented, and recorded in the ISMM

6. Transition Arrangements

For organizations with common management systems under an AOC holder, the organization shall adhere to the **SCAA's regulatory requirements** for Part-IS, including timelines and submission procedures.

As part of the transition, the organization shall:

- Conduct a Management of Change exercise;
- Submit for the review a draft of the MOE or CAME amendment (as applicable) or the Information Security Management Manual (ISMM) for independent CAMO and Part 145 AMO's not operating under a common management system;
- Submit a competence assessment of personnel performing Part-IS activities;
- Submit a manpower plan;
- Submit an updated compliance audit plan and an internal audit report;
- Submit a list of identified security hazards/risks and their associated risk levels;
- Present a suitable ISMS Assessment, using the compiled – SCAA Information Security Compliance Checklist (SCAA Form SF 58).

All required submissions must be made to the SCAA Airworthiness Inspectorate by **20 January 2026.**

Full compliance is expected by **26 February 2026**

7. Effective Date

This Notice becomes effective upon the date of issue, November 2025.

8. Enquiries

All enquiries regarding the content of this Notice should be addressed in writing to **SCAA Head of Airworthiness Mr. Giles Sicobo** at: gilessicobo@scaa.sc