



9th Meeting of the Compliance Committee (CC9) and 12th Meeting of the Parties (MoP12)

Ebene, Mauritius, 25–27 June 2025 and 30 June – 04 July 2025

MoP-12-22 / CC-09-11

Draft Terms of Reference (ToR) for a consultancy to develop the SIOFA Information System Security Policy (ISSP)

SIOFA Secretariat

Meeting	Compliance Committee ✓ Meeting of the Parties ✓
Document type	working paper ✓ information paper <input type="checkbox"/>
Distribution	Public ✓ Restricted ¹ <input type="checkbox"/> Closed session document ² <input type="checkbox"/>
Abstract	<p>This working paper presents a draft ToR for a consultant to develop the SIOFA ISSP. It includes the main objectives, tasks and deliverables requirements.</p>

¹ Restricted documents may contain confidential information. Please do not distribute restricted documents in any form without the explicit permission of the SIOFA Secretariat and the data owner(s)/provider(s).

² Documents available only to members invited to closed sessions.

Recommendations

- The MoP to review the draft ToR and amend it as required.
- The MoP to allow a budget in 2026 for the ISSP work.
- The MoP to agree to launch the call for applicant in 2026.

Draft Terms of Reference (ToR) for a consultancy to develop the SIOFA Information System Security Policy (ISSP)

Consultancy for the Development of the SIOFA Information System Security Policy (ISSP)

Project code: SEC 2025-01

1. Background

The Southern Indian Ocean Fisheries Agreement (SIOFA) is an international organization established to ensure the long-term conservation and sustainable use of fishery resources in the Southern Indian Ocean.

The SIOFA Secretariat is a small structure based in Reunion Island, and its staff consists of 4 people, one Executive Secretary and 3 Officers. Since there is no staff specialized in information technologies or cyber security, all IT-related tasks are assured by the Data Officer.

The Secretariat is in contact with many people from the SIOFA contracting parties, cooperating non-contracting parties and participating fishing entities (CCPs) and rely a lot on email for information exchanges. SIOFA usually hold 3 meetings each year which take place outside of the Secretariat, usually hosted in one CCP country. The SIOFA website is the main tool for providing information and managing meeting documents.

For achieving its objective SIOFA and the Secretariat relies on information systems to store, manage, and exchange sensitive operational, scientific, and administrative data. With growing reliance on digital platforms, cyber threats and lacks of policies may increase risks to the confidentiality, integrity, and availability of sensitive data.

To address this, SIOFA requires a comprehensive Information System Security Policy (ISSP) to provide a structured framework for information security management across all its information systems and devices.

2. Objectives

The objective of this consultancy is to:

- Develop a comprehensive and context-specific Information System Security Policy (ISSP) for SIOFA.
- Ensure that the policy aligns with international best practices and is tailored to the operational environment and mandate of SIOFA. Attention must be paid to the small size of SIOFA and its Secretariat, where there is very limited possibility to increase its budget or staffing.

- Provide recommendations for implementation, including controls, roles and responsibilities, and monitoring mechanisms.

3. Scope of Work

The consultant will undertake the following tasks:

a. Situational Analysis

Review SIOFA's current information systems, infrastructure, workflows, and existing policies.

Assess security risks and vulnerabilities in existing systems and processes, with an emphasis on sensitive information and confidential data.

Identify key stakeholders and data custodians.

b. Policy Development

Develop a ISSP including (but not limited to) the following components:

Policy objectives and scope

Governance and roles/responsibilities

Information classification and handling

Access control policies

Network and system security

Data backup and recovery

Incident response and reporting, including cyber incident and hacking

Physical and environmental security

Training and awareness

Compliance and audit

c. Consultant Engagement

Conduct consultations with SIOFA Secretariat staff and CCP to validate findings and gather input.

Present the draft policy for feedback.

d. Finalization and Handover

Incorporate feedback and submit the final version of the ISSP.

Provide an executive summary and implementation roadmap.

Deliver a short training/implementation session and a presentation for key SIOFA staff.

4. Provision by the Secretariat

The Secretariat will provide the Consultant with the following materials:

- Reports of the Data and Security audits performed in 2021-2022 (ref project SEC 2021-06).
- Current policies and procedures in place
- Current Software and IT service subscriptions

5. Deliverables

- Inception Report – outlining methodology, timeline, and consultation plan (within 2 weeks of contract signing).
- Draft Information System Security Policy.
- Secretariat and CCPs consultation report.
- Final ISSP incorporating feedback.
- Implementation roadmap and training materials.

6. Duration and Location

Duration: Up to 2 months from the signing of the contract.

Location: Remote, with potential virtual meetings with SIOFA Secretariat and other parties.

Starting Date: January 2026

7. Qualifications and Experience

The consultant (individual or company) should possess the following qualifications:

- Advanced degree in Information Security, Computer Science, or related field.
- Minimum of 5 years' experience in developing IT security policies or cybersecurity frameworks
- Demonstrated knowledge of international standards (e.g., ISO/IEC 27001, NIST). Experience working with international or intergovernmental organizations is an advantage.
- Strong analytical, communication, and writing skills.

8. Reporting and Management

The consultant will report to the Executive Secretary of SIOFA.

The consultant will also liaise with the Data Officer and the Compliance Officer for technical aspects.

9. Confidentiality

The consultant shall not release non-public data, restricted or confidential information for conducting this study to any person or any organisation, other than SIOFA Secretariat. Such information will remain the property of the SIOFA Secretariat.

The consultant shall delete all the confidential or restricted information obtained as a part of the contract immediately after the conclusion of the contract.

10. Application Requirements

The applicant(s) should submit a proposal that contains the following items:

- A current CV that summarises the applicant(s) relevant educational background and professional experience.
- A brief proposal outlining the proposed methods and analyses, including a description of how the objectives of the ToR will be achieved.
- A competitive financial proposal, SIOFA budget limit for this work is €10,000.
- Any proposed exclusions to the intellectual property clause.
- Identification of any project risks and associated mitigation and management required to successfully complete the project.
- A statement that identifies any perceived, potential, or actual conflicts of interest of the applicant(s), including those described in paragraph 4 of the SIOFA recruitment procedure (see <https://siofa.org/science/sc-guidelines>);

The applications must be submitted to Thierry Clot, Executive Secretary, thierry.clot@siofa.org by [30 November 2025].