



**TERMS OF REFERENCE (TOR) FOR
SIOFA INDEPENDENT AUDIT OF DATA SECURITY:
ACCESS, DISSEMINATION AND PRESENTATION OF DATA
Project Code: SEC2021-05**

1. Introduction

SIOFA is an intergovernmental organisation managing non-highly migratory fishery resources within the southern Indian Ocean. SIOFA is established by its constituent treaty and accountable to its decision-making body, the Meeting of the Parties.

The SIOFA Secretariat is responsible for:

- a. receiving and transmitting the official communications,
- b. facilitating the compilation and dissemination of data necessary to accomplish the objective of the Agreement,
- c. preparing administrative and other reports for the Meeting of the Parties and the Scientific and Compliance Committees,
- d. administering agreed arrangements for monitoring, control and surveillance and the provision of scientific advice,
- e. publishing the decisions of and promoting the activities of the SIOFA and its subsidiary bodies, and
- f. treasury, personnel, and other administrative functions.

SIOFA manages a range of different fisheries (see <http://www.apsoi.org>). These fisheries are generally low effort fisheries with a small number of vessels participating. This creates challenges for the access, dissemination and presentation of SIOFA fishery data to the Meeting of the Parties and subsidiary bodies and the broader public. SIOFA is seeking to ensure that commercially sensitive data remains protected and can be safely accessed for scientific and compliance purposes to ensure SIOFA fulfils its objectives.

Additionally, SIOFA is seeking two aspects: the first is to review the physical security of its data is protected against interference and other cyber threats; and the rules and procedures for access to, dissemination and presentation of data.

SIOFA does not currently have an information security policy in place.

2. Overview of the project

SIOFA is seeking an independent audit(s) of its data security. This audit comprises two parts. This consultancy is for the *Access, dissemination and presentation of data*.

Consultants are able to work remotely for this work.

Note that in parallel to this project, SIOFA will also contract a consultant to review the Physical Security of the SIOFA Secretariat. These two consultancies are independent, but the successful applicant will be required attend coordination meetings, as required, with the Secretariat to help ensure consistency in recommendations arising from the two projects.

3. Terms of Reference

The consultant will:

- Identify the full range of SIOFA datasets summarising the databases' structure and their metadata
- Design a survey for key data users taking into consideration how they interact with data and their experiences interacting with the current data holdings and protocols
- Identify, and classify issues raised and the databases/datasets in which they do or are likely to occur
- Review the existing protocols for the access, dissemination and presentation of data (including: CMM 03/2016 and any internally-developed procedures by the Secretariat. The consultant should also consider proven models from similar organisations, such as the Western and Central Pacific Fisheries Commission rules on the access and use of data, CCAMLR, SPRFMO, NAFO and IOTC)
- Document the approaches with particular attention to solutions addressing the transparency of documentation and processes involved in the data management.
- Provide advice and recommendations on improvement to these protocols, if needed, that are appropriate for SIOFA's needs and size. The consultant should give consideration to ISO/IEC 27002
- Consider options for the most appropriate way to aggregate data for presentation (taking into consideration temporal and spatial elements, and number of vessels. Options should include presentation at different scale e.g., day/year/month and set level, 1x1, 5x5, and 10x10)
- Provide draft security standards for the Secretariat and SIOFA Contracting Parties, cooperating non-Contracting Parties and participating fishing entities (collectively 'CCPs') for the use and presentation of data and annual summaries
- Prepare a workplan aiming at optimizing the access, dissemination and presentation of data showcasing the benefits of the proposed recommendations

4. Submission of information and confidentiality

- The Consultant shall submit all the information collected to the SIOFA Secretariat (including that sourced from the Secretariat) before the final payment of the contract is made to the consultant. Such information includes electronic data files, analysis codes, biological samples, and other relevant data if applicable. Any arrangements for ownership, storage, or disposal of physical samples shall be agreed by SIOFA as a part of the contract.
- All Intellectual Property generated as a part of this contract shall become the property of SIOFA unless otherwise excluded in the proposal and agreed by SIOFA in the contract. The consultant shall not release confidential data provided for conducting this study to any persons nor any organisations, other than SIOFA Secretariat.
- The consultant shall delete all the confidential data upon the completion of the contract.

5. Timeframe and reporting

The consultant is required to provide a Draft Report to the Scientific Committee meeting in 2022 by 15 February 2022.

The Consultant will take into account any feedback or concerns by the Scientific Committee and provide a Revised Draft Report to the Compliance Committee and Meeting of the Parties by 4 June 2022.

The Consultant shall provide at least one report detailing their findings in respect to the terms of reference, including clear recommendations, and an information security policy document for the access, dissemination, and presentation of data for SIOFA's consideration. These report(s) shall include at least the following:

- Detailed descriptions of the information collated and analysed,
- Data catalogue (inventory) of the information collated,
- Maps, Figures, Tables, Pictures, Diagrams, and Illustrations as much as possible to allow anyone to understand contents easily,
- Methods and detailed descriptions of analyses in a manner that allows for adequate review,
- Location and access for any data collection (datasets) that are produced from this project,
- References to relevant data and security standards
- Advice and recommendations on future work; and
- An executive summary.

6. Submission of applications

The applicants should have relevant experience of undertaking data security audits and developing data information and data security procedures for international organisations, for example “zero trust” principles, international security standards (e.g., NIST, ISO/IEC 27001, ISO/IEC 27002, ISO 31000, GDPR), and data security classification principles.

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.
- 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 <http://www.apsoi.org/scientific-committee>); and
- Any additional information the applicant(s) wish to submit.

Announcement of the call for the consultancy will be placed in the SIOFA home page in August 2021 and will be circulated to all Cooperating and Contacting Parties (CCPs).

Applications must be submitted to Thierry Clot, Executive Secretary (thierry.clot@siofa.org) by 20 September (13:00 UTC).

7. Timeline

The consultant shall follow the timeline described in Table 1 below:

Work Period	Activities
20 August – 20 September 2021	Call for the consultant through the SIOFA web site and through the circulation to Cooperating and Contacting Parties (CCPs).
21 September – 24 September 2021	Selection of the Consultant by Secretariat in consultation with Project Manager and the evaluation panel.
27 September – 30 September 2021	After selection, the Secretariat will make a contract with the Consultant. Payment milestones will be agreed through this process, and can include an upfront payment
1 October 2021 – 15 February 2022	Working period of the Consultant and submission of the data and a draft report to Secretariat. The Consultant provide a Draft Report to the Scientific Committee meeting.
15 February – 04 March 2022	Following any requests for additional works/or revisions the consultant will complete the requests and submit the final report and all information/data to the Secretariat and the Scientific Committee by 4 March 2022.
04 March – 20 March 2022	The SC Chairs and the Secretariat will review the final draft and information/data submitted. The Consultant will finalize the report and present it to the SC7.
20 March 2022 – 8 August 2022	The Consultant will take into account any feedback or concerns and provide a Revised Draft Report to the Compliance Committee and Meeting of the Parties by 4 June 2022.

8. Evaluation criteria for the selection of candidates

The selection criteria will be developed by the evaluation panel along with the project manager, the Secretariat, and the Chairpersons of the relevant subsidiary bodies. The criteria will include following items:

- Adequate submission of information to allow the panel to evaluate the candidate,
- Evaluation of the proposal from the candidate,
- Ability to undertake and complete the analyses or work required in the ToR,
- The candidate's agreement with confidentiality provisions required for the project,
- Acceptable conflict of interest statement,
- Agreement with the data submission and intellectual property terms required in this ToR, and
- Financial and resourcing considerations.

9. Contact persons

Pierre Peries, Project Manager (technical matters) pierre.peries@siofa.org

Thierry Clot, SIOFA Executive Secretary (administrative and substantial matters)

thierry.clot@siofa.org