Terms of Reference for an Independent Audit of SIOFA’s data security

Introduction

SIOFA is an intergovernmental organisation managing non-highly migratory fishery resources within the southern Indian Ocean. SIOFA is established by its constituent [treaty](https://www.apsoi.org/node/3) and accountable to its decision-making body, the Meeting of the Parties.

The 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 [*insert links to public information on SIOFA fisheries]*. These fisheries are generally low effort fisheries with a small number of vessels participating. This creates challenges for the access, dissemination and presentation of fishery data to the SIOFA 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. The two consultancies are outlined below.

Consultancy #1

SIOFA is seeking an independent audit(s) of its data security. This audit comprises two parts.

This consultancy is for the first element: *Access, dissemination and presentation of data*

Consultants are able to work remotely for this work.

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](https://www.apsoi.org/node/90) 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](https://www.wcpfc.int/administration-wcpfc-data-access-rules-and-procedures) 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 eg day/year/month and set level,1x1, 5x5 and 10x 10).
* 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

Consultancy #2

SIOFA is seeking an independent audit(s) of its data security.

This consultancy is for the first element: *Physical security*

Consultants must be able to visit the Secretariat premises to undertake this consultancy, but are able to complete the work remotely for this work.

*Physical security*

The consultant will

* Investigate the physical security of the system (including cloud-based systems) including: technical weaknesses in the security infrastructure, security risks, maintenance of confidential data, software-based security measures and user access of the database
* Consider the different sources of data (logbook, observer, VMS) and options to mitigate any security risks in the transmission of that data.
* Review how, when and where data is stored and backed up
* Information and data classifications
* Consider:
  + lines of responsibility and control
  + access authorization
  + user account approval
  + account creation and termination
  + user identification and authentication
  + core systems application administration, including roles of Secretariat staff
  + email and webmail
  + use and accountability for SIOFA Secretariat ICT assets
  + monitoring and reporting
  + user needs (both Secretariat and CCPs)
* Provide best security practises to implement at SIOFA’s Secretariat
* Recommend any building, hardware, software and database upgrades as necessary.
* Prepare an information security policy for SIOFA’s consideration

*Timeframe*

*The consultant is required to provide a Draft Report to the Scientific Committee meeting in 2022 (due 15 February 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 in June 2022.*

All tenders must be submitted via email and received by the [date] Reunion time.

No late submissions will be considered.

Requests for additional information relating to this consultancy and submissions of bids should be directed to: [insert]