An Indian Ocean Tuna Commission Pilot Project on Vessel Monitoring System

1st Interim report: Proposal, Design and Requirements of the IOTC VMS Pilot Project

AN INDIAN OCEAN TUNA COMMISSION PILOT PROJECT ON VESSEL MONITORING SYSTEM

December 20, 2024

Anthony UBERTI
RENASCENTIA CS

A. Executive Summary

In the frame of the contract service with reference COI/Ecofish/CT/2024/356 named “An Indian Ocean Tuna Commission Pilot Project on Vessel Monitoring System,” this report is the second deliverable and the first interim report. It aims to establish the technical requirements and Standard Operating Procedures (SOPs) for designing the IOTC Regional Vessel Monitoring System (VMS) Pilot Project.

The **1st Interim Report on the IOTC VMS Pilot Project** provides a detailed roadmap for implementing a regional VMS Pilot System to strengthen fisheries governance and combat illegal, unreported, and unregulated (IUU) fishing. It emphasizes the critical importance of enhanced monitoring, compliance, and regional cooperation to ensure the sustainable management of tuna and tuna-like species in the Indian Ocean.

The pilot project focuses on testing two reporting models—**shared decentralized** and **partially centralized systems**—while prioritizing real-time data collection, secure data governance, and system interoperability. The report underscores the need for alignment with international standards, robust regional cooperation, and stringent data security protocols supported by scalable, cloud-based solutions.

This initiative aims to enhance enforcement capabilities, streamline data sharing, and promote harmonized practices to support sustainable fisheries management. It highlights the importance of stakeholder engagement, with well-defined roles and responsibilities. The report also recommends structured operational procedures, targeted training programs, and mechanisms for continuous improvement to ensure the success of the pilot.

The outcomes of this project will establish key milestones and lay the foundation for developing a state-of-the-art Regional VMS System in the Indian Ocean.

B. IOTC VMS PILOT PROJECT GUIDELINES

I. Introduction

The Indian Ocean Tuna Commission (**IOTC**) is responsible for the management of tuna and other tuna-like species within the Indian Ocean region, which spans vast areas of international waters, national exclusive economic zones (**EEZs**), and high seas. Given the migratory nature of these species and their economic importance, the IOTC plays a crucial role in ensuring their sustainable exploitation. One of the main challenges to fisheries management in the region is the enforcement of rules against Illegal, Unreported, and Unregulated (**IUU**) fishing, which threatens the ecological balance and depletes valuable fish stocks. However, as highlighted in various IOTC sessions and working group reports, existing VMS frameworks face challenges such as inconsistent standards, limited data sharing, and variable implementation across Contracting Parties (**CPCs**).

To address these issues and develop a more robust VMS framework, the IOTC and its VMS Steering Group launched discussions starting in 2019 for the implementation of a regional Vessel Monitoring System (VMS), which will serve as a critical tool for monitoring fishing vessels' activities. VMS enables the tracking of vessels' location and movement through satellite or other tracking technologies, thus supporting enforcement and monitoring activities. Therefore, in order to reach this goal, the decision taken to set up a VMS Pilot Project is a significant step forward putting in line IOTC's monitoring efforts and international best practices. This proposed Regional VMS Pilot Project will trial two distinct reporting methods— Shared Decentralized and Partially Centralized—across participating Contracting Parties and Cooperating Non-Contracting Parties (Volunteer CPCs).

This project aims to evaluate the effectiveness of these methods in improving compliance with fisheries regulations, detecting violations of conservation measures, and enhancing cooperation among CPCs. Furthermore, the project will explore the feasibility of implementing VMS on a region-wide scale, building a framework that can be adopted by all IOTC members in the future.

II. Objectives and Scope of the IOTC VMS Pilot Project

1. Objectives

The IOTC VMS Pilot Project is a starting point and the first step, and it needs to be designed and implemented with the goal to achieve critical objectives that address both current challenges and future needs in vessel monitoring, enforcement, and fisheries management within the IOTC area of competence.

1.1 Enhance Monitoring and Enforcement to Combat IUU Fishing

Illegal, unreported, and unregulated (**IUU**) fishing poses a significant threat to the sustainability of marine resources and the economic viability of fisheries. The VMS pilot project aims to:

- **Increase surveillance coverage** across the high seas and national EEZs to identify and deter unauthorized fishing activities.
- **Provide real-time alerts and data** to support rapid enforcement actions by CPCs.
- **Strengthen Oversight:** Equip the IOTC Secretariat with tools to monitor and analyze VMS data.
- **Improve compliance** with IOTC conservation and management measures (**CMMs**) through robust tracking and reporting mechanisms.

1.2 Strengthening Cooperation and Coordination among CPCs

- **Facilitating Dat Exchange**: Establishing protocols for seamless data sharing between coastal, flag and inspecting CPCs.
- **Promoting Joint MCS Efforts**: Provide a regional surveillance VMS Platform to encourage the pooling of resources to operate coordinated patrols, inspections and investigations this, in order to enforce IOTC measures.
- **Building Mutual Trust**: Developing transparent data-sharing agreements that respect confidentiality while fostering cooperation.

1.3 Increase Transparency among CPCs and the IOTC Secretariat

Transparency is critical to fostering accountability and promoting a level playing field in the control of fishing activities. This VMS pilot project will:

- **Rationalize Reporting:** Through the testing of the different reporting options (**2 & 3 and hybrid approach**), the objective will be to ensure consistent data submissions from first, Volunteer CPCs and later from all CPCs to reduce discrepancies.
- **Improve Access to Data**: Facilitate access to VMS data by the sharing and the dissemination of the VMS data and also by giving a direct access to the Pilot VMS Platform through the creation and management of user accounts (with specific user accounts rights of access).

1.4 Test Interoperability Based on different Scenarios

With Volunteer CPCs operating diverse FMC systems and VMS transponders, ensuring interoperability is crucial. The pilot will contemplate different reporting scenarios:

- **Shared Decentralized architecture**: Data is retrieved and managed by Volunteer CPCs systems and shared with the IOTC Secretariat.
- **Partially Centralized architecture**: Data is transmitted directly from the Vessels to the IOTC Secretariat through direct connection to Mobile Communication Service Provider (**MCSP**).
- **Hybrid architecture**: A combination of both Shared Decentralized and Partially Centralized architectures.

1.5 Develop IOTC Standardized rules for Data Sharing, Confidentiality and Security

Data sharing is essential for effective regional monitoring, but it must be done securely and consistently. The project will:

- **Establish Protocols**: Define rules for data sharing, use and protection, respecting confidentiality

- **Standardize protocols** for data sharing across Volunteer CPCs and with the IOTC Secretariat.
- **Adopt Security Measures**: Implement access control to safeguard sensitive information.
- **Promote Consistency**: Align Volunteer CPCs practices with the agreed protocols to reduce variability in implementation.

1.6 Evaluate the Technical feasibility of a Regional VMS system

Implementing a regional Vessel Monitoring System (**VMS**) requires assessing its capacity to meet IOTC's monitoring and compliance needs while addressing the diverse operational requirements of CPCs. Volunteer CPCs will play a pivotal role in evaluating the pilot system. Key aspects include:

- **System Compatibility and Integration**: Analyze how existing National VMS frameworks can meet and interface to IOTC VMS regional system. This involves compatibility with different software architectures, communication protocols and data formats exchanged.
- **Infrastructure Requirements**: Identify hardware, software and network infrastructure necessary to support real-time data collection, processing and dissemination.
- **User functionalities and User Interface**: Validate and confirm the set of tools and functionalities required to allow displaying and working with the VMS data.
- **Scalability and Performance**: Examine the VMS pilot system to treat and process an increasing data volume as the number of monitored vessels will grow in its final implementation phase (after the piloting phase). Evaluate performance metrics such as data latency, accuracy and reliability under different operational conditions.
- **Technical Support and Training**: Evaluate the need for capacity building, training and ongoing technical support for stakeholders.
- **Cybersecurity and Data Protection**: During this pilot project, objective will be to assess and evaluate the measures needed to safeguard sensitive information against cyber threats and unauthorized use. Develop procedures and protocols for secure data transmission and access control.

By addressing these factors, the pilot will provide a solid foundation for scaling up to a fully operational and efficient regional VMS Center in the next phase.

2. Scope of the IOTC Pilot Project

The IOTC VMS Pilot Project aims to establish and test a comprehensive framework for vessel monitoring, targeting various categories of fishing and non-fishing vessels within the IOTC area of competence. In alignment with IOTC Resolution 15/03 and its proposed amendments, the pilot project will define key parameters, including vessel scope, area of interest, data content, reporting frequency, and protocols for VMS data sharing among stakeholders.

2.1 Geographical AOI

The pilot project will cover the entire **IOTC area of competence**, including the **high seas**, **coastal zones**, and **exclusive economic zones (EEZs)** of Volunteer CPCs. The IOTC has jurisdiction over the conservation and management of tuna and tuna-like species in these areas, and the VMS system will provide a mechanism for monitoring vessels operating within both national and international waters. The pilot will ensure that the VMS system is capable of tracking vessels across different geographical areas, including those that operate in close proximity to coastal zones and others that engage in high seas fishing.

2.2 Targeted Vessels

The VMS Pilot Project will apply to the following vessel categories among the possibilities offered by the Volunteer CPCs fleets:
At least according to IOTC **Resolution 15/03:**

- **Fishing Vessels ≥24m LOA**: All vessels flagged under CPCs operating within and beyond their Exclusive Economic Zones (**EEZs**).
- **Fishing Vessels <24m LOA operating beyond Exclusive Economic Zones (EEZs):** Smaller vessels operating on the high seas

And potentially to a broader vessel sample according to IOTC **Res 15/03** proposed amendments as follows:

- **Carrier and Support Vessels:** Vessels that transport catches or provide logistical support to fishing operations, including bunker and supply vessels.

- **Fishing Vessels <24m LOA within EEZs:** Among the Volunteer CPCs that would agree to include a broader range of vessels, selected smaller vessels within EEZs, particularly those identified as being involved in high-risk activities or operating in sensitive areas, may also be included, aligned with proposed amendments to Resolution 15/03.

2.3 VMS Data contents and reporting frequency

The pilot project will focus on VMS-only data, transmitted at least once every **four hours** but preferably once **every two hours**, with the following regular data reporting specifications:

- **Vessel Identification (ID) :** Unique identifier for the vessel.
- **Current Geographical Position**: Latitude and longitude with a position error not exceeding 50 meters at a 99% confidence level.
- **Speed and Course:** in knot and degree
- **Date & Time (UTC)** of the position fix.
- **Event Codes:** Event codes to be received and treated by the system if the MTU unit brings these possibilities:
  - Power UP/DOWN alerts.
  - Antenna block/obstructed alerts (satellite- or GSM-based).
  - Automatic alerts for intrusion/tampering detection (e.g., if the VMS unit is opened).
  - Entry/Exit zone alerts.

This data will provide a comprehensive overview of vessel activities, enhancing monitoring and compliance efforts within the IOTC area of competence.

Command Features for the Pilot Project

The VMS system will support the following commands:

- **Polling Command**: Enables real-time location requests from vessels.

2.3.1 Near Real-Time Transmission

In the frame of this Pilot Project, each VMS Data transmission will have to be executed in near real-time, automatically through **MtoM** mechanism and without any alteration.

2.4 VMS Data Sharing Protocol

According to **IOTC-2024-CoC21-11(E)**, development of rules and procedures for the sharing, use and protection of VMS data remain pending. However, the VMS Pilot Project will be a good tool to progress on related discussion and should clarify the path toward the task of elaborating an agreement on the IOTC VMS Data Sharing Protocol. This project will be also a good opportunity to test and validate Resolution 15/03 proposed amendments as outlined in the document **IOTC-2023-VMSWG06-03.**

Accordingly, the **VMS Data sharing strategy** between Volunteer CPCs and IOTC secretariat will test different scenarios.

2.5 Different Scenarios to be tested

The VMS Pilot Project will evaluate various scenarios to determine the technical feasibility of implementing a Regional VMS System. These scenarios are categorized into two main areas: **data collection** and **data distribution**.

2.5.1 The collection of VMS Data- VMS Data Transmission from Volunteer CPCs to IOTC Secretariat

- VMS data contents as required according to section 2.3
- According to option "**Shared Decentralized**" from the Volunteer CPC Fisheries Monitoring Centre (**FMC**) to IOTC VMS Regional Pilot Platform (**Scenario 1**).
- According to option "**Partially Centralized**" from the Mobile Communication Service Provider of the Volunteer CPCs flagged vessels to IOTC Secretariat (**Scenario 2**).

2.5.2 The Distribution of the VMS Data- VMS Data Transmission from IOTC Secretariat to Volunteer CPCs

Two options will be available for this Data distribution:

- The IOTC Regional VMS Pilot Platform will route the VMS data collected through automatic data delivery mechanism to Volunteer CPCs FMC system (**Scenario 3**). This data sharing will be operated according to rules of data sharing that will be integrated into the Pilot Platform.
- VMS data available directly from the Regional VMS Pilot Web-based User Interface for the Volunteer CPCs (**Scenario 4**). This Data access will be regulated through user accounts on the Pilot Platform with specific restrictions:
    - Per vessel or group of vessels.
    - Per designated area.
    - Limited to specific time periods.
    - With Expiry date

3. VMS Overview

A thorough understanding of the existing VMS ecosystem within the IOTC jurisdiction is essential for the successful design and implementation of the IOTC VMS Pilot Project. This includes analyzing state-of-the-art systems currently in use within the IOTC area of competence to assess the overall level of VMS compliance among CPCs. Specifically, evaluating the capacities of Volunteer CPCs in terms of VMS compliance and data exchange capabilities is critical to the project's success. Finally, incorporating best practices from other RFMOs in regional VMS cooperation could provide valuable insights and key drivers to align with the most effective regional VMS strategies.

3.1 IOTC CPCs VMS Overview

Based on the study of the 2022 VMS adoption and report documents for each IOTC CPC, a summary table is available in appendix. This table consolidates key information on the level of VMS compliance among CPCs, the types of systems used, and their technical capabilities, including data transmission intervals and failure reporting methods. It also highlights vessels >= 24 meters LAO and vessels operating outside EEZs and their VMS adoption, providing insights into the readiness of CPCs to participate in the pilot project.

This overview establishes a baseline for identifying gaps, evaluating volunteer CPC capacities.

Main highlights can be summarized as follows:

- **FMC (Fisheries Monitoring Centers):** All surveyed CPCs reported the existence of operational FMCs, indicating a baseline capacity for monitoring.
- **VMS Systems in Use:** A variety of satellite systems are deployed, including **Inmarsat**, **Iridium**, **Orbcomm**, and **Global Star** meaning the high flexibility need of the Regional VMS System.
- **Transmission Intervals and Reporting:** Most CPCs report data at **hourly intervals**, showing robust monitoring capabilities and area for improvement.
- **Vessels with Satellite VMS: 70% compliance for vessels ≥24m and 75% compliance for vessels < 24m operating outside EEZ** which launch a good baseline for implementing a Regional VMS.

The analysis of 2022 VMS adoption highlights a strong foundation for the IOTC VMS Pilot Project, with operational FMCs across all CPCs, diverse satellite systems ensuring flexibility, and high compliance for vessels ≥24m and those operating outside EEZs.

3.2 Volunteer CPCs Overwiew

For conducting this Pilot project, following CPC have confirmed their will to participate to that project:

- **AUSTRALIE**
- **THE PHILIPPINES**
- **SEYCHELLES**

In order to collect the technical information needed for preparing this VMS Pilot project, a questionnaire was submitted to those Volunteer CPCs (**see appendix**), below are main information categories that was intent to be collected:

- **Fleet Segmentation:**
    - Questions align with IOTC Resolution 15/03 to categorize fleets based on vessel size and activity area.

- **VMS Providers and Technologies:**
    - Identification of Mobile Transmitting Unit (**MTU**) VMS providers used by Volunteer CPCs.
    - Assessment of advanced features such as geofencing capabilities and automated data exchange.
- **Service Provider Capabilities:**
    - Evaluation of the ability of VMS service providers to transmit data directly to regional centers.
- **VMS Data Format and Data exchange:**
    - Ensuring compliance with standardized data formats and exchange protocols.

The following is the information gathered from the Volunteer CPCs:

3.2.1 AUSTRALIA

- MTU approved and used for the segment fleet under the scope of the VMS Pilot project:

MTUs	Communication Technologies
Skywave IDP-690	**Orbcomm IsatDataPro**
Skywave IDP ST 6100	**Orbcomm IsatDataPro**
Skywave IDP ST 9100	**Orbcomm IsatDataPro**
CLS TRITON ADVANCED	**IRIDIUM SBD**

- Reporting Method chosen = **Option 3 - Partially Centralized**.
- VMS Data Format supported by MCSPs operating in AUSTRALIA:
    - Data formats supported: Excel -csv / Naf / FLUX
    - Communication protocols supported: ftp /Https POST
    - Polling response capacity = YES

3.3 RFMOs Regional VMS benchmark

Based on the **ISSF Technical Report 2022-06 RFMO VESSEL MONITORING SYSTEMS** document review, below are relevant highlights that should be considered and integrated in IOTC Secretariat reflections for the set-up to this VMS pilot project:

- **Centralized Reporting**: Centralized systems, such as those of **WCPFC** and **SPRFMO**, demonstrate the efficiency of simultaneous reporting to the RFMO Secretariat and flag states, ensuring real-time monitoring and transparency. Semi-centralized approaches, combining national **FMCs** with RFMO direct data collection, offer adaptable solutions.
- **Harmonized Standards**: Standardized data formats and communication protocols, like the North Atlantic Format used by ICCAT and NAFO, enhance interoperability. Harmonization ensures seamless data exchange between CPCs and minimizes operational complexities.
- **Enhanced Compliance Monitoring**: Frequent reporting intervals (**e.g., 1–4 hours**) and tamper-proof MTUs, as mandated by most RFMOs, strengthen compliance and data integrity. Robust rules for handling technical failures further ensure reliability.
- **Scientific Utility**: Allowing VMS data for scientific purposes, as done by **ICCAT** and **WCPFC**, supports conservation planning and stock assessments. Historical VMS data sharing with scientific committees ensures long-term benefits while maintaining confidentiality.

These benchmarks provide a solid foundation for the IOTC Secretariat to design a reliable, adaptable, and effective VMS pilot project.

C. Design of the IOTC Pilot Project on VMS

This chapter outlines the design framework for the IOTC Vessel Monitoring System (**VMS**) Pilot Project. It integrates insights from international best practices and aligns with the Information System Value Chain approach, addressing data acquisition, processing, storage, security, and distribution. The primary objective is to establish a scalable, secure, and interoperable system capable of real-time monitoring of fishing vessels in the IOTC area of competence that can serve as foundation for VMS Regional implementation later on.

I. Overview of the System Design

The IOTC Pilot Project on VMS aims to improve the monitoring, control, and surveillance (**MCS**) of fishing activities within the IOTC area of competence. By leveraging advanced technologies and harmonized data-sharing protocols, the project seeks to enhance compliance with conservation and management measures, strengthen regional cooperation, and provide actionable insights for sustainable fisheries management.

1. System Value Chain Components

The IOTC VMS Pilot Project is built upon the principles of the Information System Value Chain, ensuring an end-to-end solution that integrates key functionalities for effective monitoring and management. The components include:

- **Data Collection:** This involves the continuous acquisition of real-time positional data from multiple Mobile Transmitting Units (**MTUs**) Providers. The system should ensure seamless communication using industry-standard communication protocols for secure and reliable data transmission. The Pilot Platform shall also integrate main International VMS data format standards.
- **Data Processing:** Collected data shall undergo validation to ensure accuracy and integrity. Automated systems will analyze and flag key events such as geofence events, tampering, and unauthorized activities. Analytical tools will operate to derive actionable

insights, including historical trajectory analysis and fleet behavior patterns, to support decision-making.

- **Data Storage:** Scalable storage infrastructure will be implemented to house historical and current data. The system shall ensure data redundancy through advanced backup mechanisms, such as daily incremental and weekly full backups, adhering to international standards like **ISO 27001** and **ISO 27002** for data integrity and security.
- **Data Distribution:** The system will provide a controlled and flexible framework for sharing validated data among stakeholders, including Volunteer CPCs. Secure communication protocols and APIs shall enable integration with third systems, while custom configurations will allow data to be filtered by vessel, zone, or time frame. The system will support multiple formats for ensuring high interoperability level with third systems.
- **User Interface:** A user-centric approach shall ensure that the interface offers intuitive dashboards, interactive mapping tools, and real-time alerts. Customizable views and notifications will allow stakeholders to tailor their experience to specific monitoring needs.
- **Security and Confidentiality:** Robust encryption mechanisms will secure data during transit. Role-based access control, combined with solid authentication, will restrict unauthorized access, while efficient and complete Auditing tool will log and alert on any activity proceed on the data. These measures will ensure that the system complies with IOTC **Resolution 15/03** and global data protection standards.

2. System Design and Technical requirements

2.1 System Design

According to discussion taken in the IOTC VMS Working group based on the VMS Study *IOTC-2019-WPICMM02-VMS_Study[E]*, two options of reporting methods have been selected as two scenarios needed to be tested during the pilot project.

A quick reminder on the mentioned methods can be found below:

Option 2: "Shared Decentralized "

- **Key Features**:
    - Data collected by the CPCs is shared with the IOTC Secretariat and other relevant CPCs under specific guidelines.
    - The CPC's Fisheries Monitoring Center (**FMC**) plays a central role in gathering and disseminating data, ensuring real-time data flow to stakeholders based on agreed protocols.
    - Transparency increases, as sharing rules enforce standardization and allow for broader access to VMS data among CPCs.
- **Advantages**:
    - Builds on existing national systems, minimizing the need for infrastructure overhaul.
    - Costs are relatively manageable, as the CPCs maintain accountability for VMS management, with the Secretariat only requiring infrastructure for data reception and limited processing.
    - Allows coastal states to access relevant data on vessels operating in their EEZs, fostering compliance with territorial regulations.
- **Challenges**:
    - Requires rigorous data-sharing agreements to ensure timely and consistent data exchange.
    - Depends heavily on the capacity of CPC FMCs to manage and transmit data, which could lead to delays or inconsistencies.

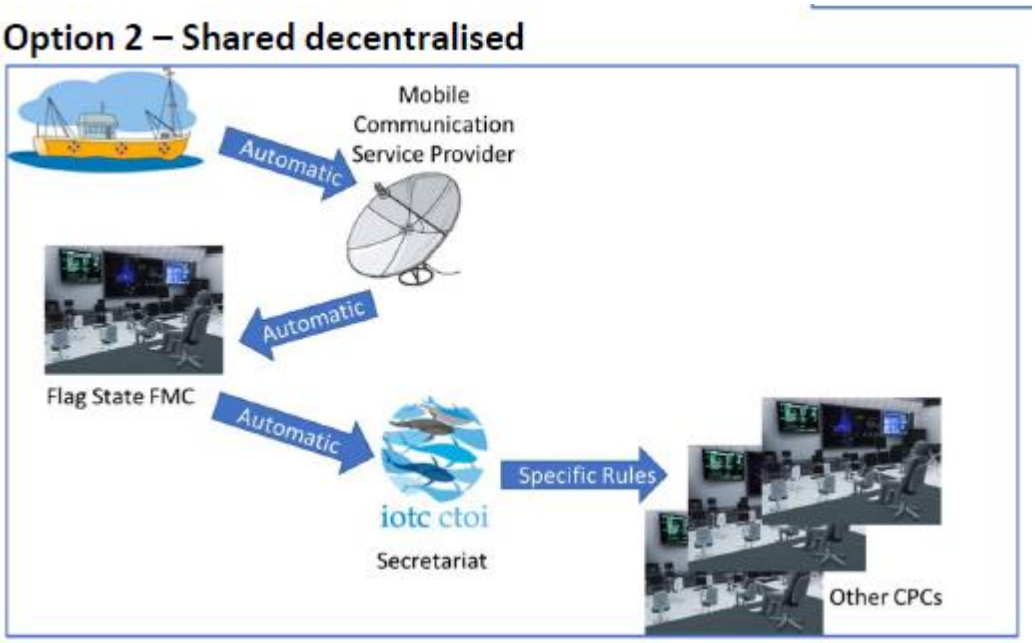

Figure 1: IOTC-2019-WPICMM02-VMS Study[E] - "Shared Decentralized".

Option 3: Partially Centralized

- **Key Features**:
  - VMS data is transmitted directly from the Mobile Communication Service Providers to the IOTC Secretariat, bypassing CPC FMCs.
  - The Secretariat becomes the central repository and manager of VMS data, enabling seamless and standardized data access for CPCs.
- **Advantages**:
  - Enhanced real-time monitoring and data reliability, as data flows directly to the Secretariat without potential filtering or delays.
  - Greater transparency in compliance monitoring and enforcement, as all stakeholders receive the same data.
  - Simplifies implementation for CPCs with limited resources by reducing their VMS management burden.

- **Challenges**:

  - Initial setup costs are higher for the Secretariat due to the need for robust infrastructure and staffing.
  - Legal and operational frameworks for centralized data access and sharing must be well-defined and regionally accepted.

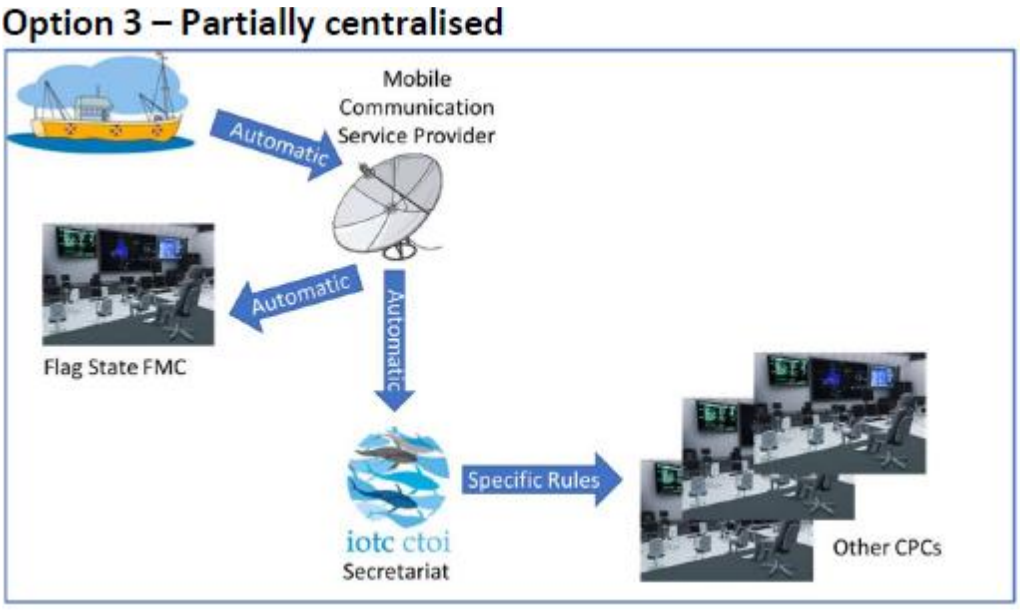

Figure 2: IOTC-2019-WPICMM02-VMS Study[E] - "Partially Centralized".

The evolving complexities of vessel monitoring at regional scale and the need for real-time, reliability, and accessible data demand innovative approaches that leverage the strengths of both centralized and decentralized systems. While Option 2 (**Shared Decentralized**) builds on the existing capacities of CPCs, it faces limitations in ensuring uniformity, timeliness, and data transparency. Conversely, Option 3 (**Partially Centralized**) offers improved real-time data accessibility and consistency but requires significant investment and structural changes.

To bridge these gaps, an **hybrid reporting strategy** emerges as a practical and forward-looking solution. This approach combines the efficiency and standardization of centralization with the flexibility and cost-effectiveness of decentralized systems. By blending these models, the hybrid strategy addresses the diverse needs of CPCs, facilitates incremental implementation, and ensures broader adoption while maintaining compliance with existing IOTC frameworks.

Hybrid Reporting System

- **Key Features:**
  - **Dual Data Flow**:
    - Combines CPC-based FMCs and direct reporting from Mobile Communication Satellite Providers to the IOTC Secretariat.
    - Allows data transmission flexibility based on vessel type, area of operation, and CPC readiness.
  - **Standardization Across Systems**:
    - Establishes uniform protocols for data transmission, access, and confidentiality.
    - Ensures compatibility of diverse VMS technologies and reporting systems.
  - **Enhanced Accessibility**:
    - Provides CPCs with access to both centralized and national datasets, enhancing operational flexibility.
  - **Advantages:**
    - **Cost-Efficiency**:
      - Leverages existing CPC infrastructure, reducing upfront investment in centralized systems.
      - Optimizes operational costs by utilizing scalable, cloud-based solutions.
    - **Transparency**:
      - Facilitates near real-time monitoring and data sharing, improving compliance and oversight.
      - Reduces delays and potential data filtering by bypassing national FMCs for direct reporting.

- **Scalability**:
  - Adaptable to future needs, such as expanded vessel coverage, additional monitoring tools, and advanced analytics.
- **Risk Mitigation**:
  - Ensure continuity by maintaining decentralized backups in case of centralized system failures.

- **Challenges:**
  - **Data Standardization**:
    - Harmonizing diverse VMS protocols, formats, and technologies used by CPCs requires significant effort.
  - **Legal and Policy Frameworks**:
    - Developing agreements on data access, confidentiality, and sharing between CPCs and the Secretariat can be time intensive.
  - **Infrastructure and Capacity Gaps**:
    - CPCs without FMCs or modern VMS capabilities may require technical assistance and funding.
  - **Incremental Costs**:
    - While cost-efficient overall, hybrid implementation still involves upfront investments in software, training, and pilot testing.
  - **Coordination Complexity**:
    - Managing dual reporting channels demands clear governance and robust monitoring mechanisms.

The **hybrid reporting method** strikes a balance between innovation and pragmatism, offering a structured yet flexible path for advancing the IOTC VMS Pilot Project. By addressing these key features, advantages, and challenges, the hybrid strategy can ensure robust and sustainable monitoring capabilities across the Indian Ocean region.

Aligning with option 2 scenario 1 and option 3 scenario 2 (refers to Scope section), the Hybrid IOTC VMS Pilot Platform will have to integrate multiple APIs, VMS

data formats and communication protocols to ensure high interoperability with the different VMS data senders (MCSP, FMCs and potentially RFMOs).

2.2 Data Collection and Transmission

In order to ensure proper Vessel Monitoring system, the system Database shall handle both **Declarative Data and Dynamic Positioning Data**. Minimum information and data inputs can be resumed as follow:

- **Positional Data Report**
- **Record Authorization Vessel (RAV) Data fields**
- **Additional dataset proposal**

2.2.1 Dynamic Positioning Data

Whatever the reporting method (option 2 or 3), the Piloting System Database will have to handle the following **VMS Data fields**:

Positional Data Report

- **Message Type:** (Regular report, Manual report, event generated report, ***Response to poll only for Option 3***)
- **Country Code /Flag State**
- **MTU ID:** ID of the VMS Transceiver
- **Vessel Identification (ID) :** Vessel Name/ Radio Call Sign
- **Current Geographical Position**: Latitude and longitude with a position error not exceeding 50 meters at a 99% confidence level.
- **Speed (in knots) and Course (in degrees)**
- **Date & Time (UTC)** of the position fix.
- **Event Codes:** Event codes to be received and treated by the system if the MTU brings these possibilities:
    - Power UP/DOWN alerts.
    - Antenna block/obstructed alerts (satellite- or GSM-based).

- Automatic alerts for intrusion/tampering detection (e.g., if the VMS unit is opened).
- Entry/Exit zone alerts.

Additionally, The System **Database** will have to collect either automatically (trough Synchronization) or through manual declaration the following information.

2.2.2 Declarative Data

The data fields of IOTC Record Authorization Vessels (**RAV**) file shall be the minimum information requirements that the IOTC VMS Pilot System Database shall handle.

Below is table resuming this information.

Data Field	Explanation
IOTC Number	Unique identifier assigned to the vessel in the IOTC Record of Authorized Vessels (RAV).
Type	Type or classification of the vessel (e.g., fishing vessel, support vessel).
Name	The registered name of the vessel.
Flag State	The country under whose jurisdiction the vessel is registered.
Range	The operational range of the vessel (maximum distance it can travel without refueling).
REGNO	Registration number assigned by the flag state authority.
IMO	International Maritime Organization number for vessel identification (if applicable).
IRCS	International Radio Call Sign used for communication purposes.
Port	Port where the vessel is registered or based.
Vessel Kind	The category or type of vessel, such as purse seiner, longliner, or trawler.
Gears	Type of fishing gear used by the vessel (e.g., longline, gillnet, purse seine).

LOA (m)	Length Overall of the vessel in meters, measuring the total length from bow to stern.
GT (Gross Tonnage)	A standardized measure of the vessel's internal volume, used for regulatory purposes.
GRT (Gross Registered Tonnage)	Older volume measurement system based on registered spaces within the vessel.
Total Volume (m^3)	Physical total cubic volume of the vessel's enclosed spaces.
CC (MT)	Carrying Capacity in metric tons (MT), indicating the vessel's maximum payload.
Owner	Name of the vessel's owner.
Owner Address	Address of the vessel owner.
Operator	Name of the person or entity operating the vessel.
Operator Address	Address of the vessel operator.
Operating Company	Company responsible for the vessel's operations (if applicable).
Operating Company Address	Address of the operating company.
Operating Company Reg Num	Registration number of the operating company.
Beneficial Owner	The ultimate individual or entity that benefits from the ownership of the vessel.
Beneficial Owner Address	Address of the beneficial owner.
From	Start date of the authorization period.
To	End date of the authorization period.
Starboard Photo	Photo of the vessel's **starboard side** (right side).
Portside Photo	Photo of the vessel's **port side** (left side).
Bow Photo	Photo of the **front (bow)** section of the vessel.

Last Updated	The date when the vessel information was last updated in the RAV.

Table 1: IOTC Record Authorization Vessels (RAV) data fields

Additional Declarative Data could be considered for this Pilot project as proposed in the table below:

Proposed Data Field	Explanation	Purpose/Benefit
Fishing License Details	Information on the vessel's fishing license, including license number, validity period, and authorized fishing areas.	Ensures vessels are licensed for their operations and clarifies compliance scope.
Mobile Transmitting Unit (MTU) Details	Information on VMS equipment, including manufacturer, model, serial number, and communication provider.	Ensures vessels have compliant and traceable VMS devices for real-time monitoring.
Status of Authorization	Indicates whether the vessel's authorization is Active, Suspended, or Expired.	Provides clarity on the vessel's operational status to prevent unauthorized fishing.
Home Port	The vessel's base port where it typically returns for docking, refueling, or resupplying.	Helps identify the vessel's operational patterns and flag state jurisdiction.
Contact Email	Email address for the vessel owner/operator.	Facilitates direct communication for monitoring, compliance, or inspections.
Contact Telephone	Telephone number for the vessel owner/operator.	Ensures quick communication, particularly in case of emergencies or verification.
VMS Reporting Frequency	Specifies the required interval for VMS data transmissions (e.g., every 2 hours).	Supports compliance with VMS reporting requirements (e.g., Res 15/03 amendments). Moreover, it permits to configure Overdue report alarm.
Date of Entry into RAV	The date the vessel was added to the Record of Authorized Vessels.	Improves tracking of when the vessel became authorized under IOTC regulations.

Deactivation Date	The date when the vessel was deactivated or removed from the RAV.	Provides historical tracking and helps avoid unauthorized activity post-expiry.
Geographical Objects (GO)	Information on geographical objects, including GO Type (Official/User Zones, marks, Ports), GO Ref, and Active Period (if seasonal).	Supports spatial monitoring and ensures compliance in authorized fishing areas.
System User Account Information	User account details, including User ID, Full Name, Organization, Role and Permissions, Contact Information, Login Credentials, and Language Preferences.	Enhance system security, role-based access control, and user accountability.
Operational Notes	Free-text field for comments on vessel activity, inspections, or irregularities.	Allows for additional monitoring insights and observations.

Table 2: Additional data fields proposal

This information combined with the VMS data will help to operate a State-Of-The-Art surveillance and fishing activities monitoring into IOTC area of competence.

2.2.3 Data Integrity

In order to ensure data traceability and integrity, the System should record all changes made to critical data including:

- **Vessel Data**: Creation, edits, and deletions of vessel details.
- **Spatial Data**: Modifications to geographic objects.
- **User Accounts**: Updates to roles, permissions, and account details.
- **Vessel Groups and Alerts**: Adjustments to group configurations and related alerts.
- **Poll Requests**: Logs changes related to positional data queries.
- **Device Details**: Tracks historical device allocations to vessels and updates.

Audit reports in a user-friendly and readable format should be available and exportable into Excel format.

2.2.4 VMS Data Formats

It is the structure and encoding of the data transmitted either by the Vessel MTU MCSP or by Vessel National FMC. It defines how the information will be organized, stored, and interpreted into the IOTC VMS Pilot System. Using standard VMS Data formats will ensure the data to be read and understood consistently by the VMS Pilot Platform. Therefore, the VMS data formats to be considered as a minimum for this pilot project should be the following:

- **NAF** (**North Atlantic Format**): Used for exchanging fisheries-related data between organizations.
- **XML** (**eXtensible Markup Language**): A flexible, structured format widely used for interoperability.
- **XML-Based FLUX P1007 :** A UN/CEFACT standard specifically designed for fisheries data exchange including VMS data.
- **JSON** (**JavaScript Object Notation**): A lightweight, human-readable format for data exchange.
- **CSV** (**Comma-Separated Values**): A simpler format for tabular data.

Managing these formats will ensure high interoperability and will make system Independent of the SCS technologies used to send the data.

The case of Inmarsat C/ Mini-C

For some old MTUs systems working with INMARSAT, it might be possible that the data should be retrieved directly from the LES (**Land Earth Station**). In this condition, the IOTC VMS Pilot System should manage correct API to collect the VMS encrypted data from LES, addressing legacy system needs. With the rising cost of INMARSAT, the proportion of MTU working with this SCS tends to decrease but it is most likely that the number of legacy systems using this SCS technology is still critical and needs to be considered. Therefore, the VMS solution selected by IOTC secretariat for the VMS pilot Project should integrate INMARSAT APIs and be able to retrieve data directly from the Inmarsat LES.

If we look to neighbor RFMO like WCFC, based on its list of approved Mobile Transceiver Units (MTU)/Automatic Location Communicators (ALC) dated from 06 February 2024, we can see that there are still a huge number of Inmarsat C/mini-C legacy models:

- **FELCOM10/12/15/16/18/19**
- **JUE-75C/75C-FFA/85/87/95C/95VM**
- **ELB2000/ELB2004**
- **SAILOR 3027D/6140/6150**
- **TT-3020C/3022D/3026/3026D/3026S /3027M/3062D**
- **TNL7001/7002/8001/7005**

It should be wise to validate that potential system provider is compatible with above VMS MTUs to avoid technical dead end during the operational phase after the Pilot Project.

2.2.5 Communication Protocols

As see below, VMS data should be transmitted in standard formats, such as **NAF**, **XML**, **JSON**, or **CSV**, using secure communication protocols including **HTTPS (POST or GET)**, **SFTP***, **RESTful Apis** (for **JSON** format) **and SOAP v1.2** with two-way SSL (For **P1007 FLUX**).

Moreover, Data shall be encrypted using encryption mechanism TLS 1.3 standard with TLS 1.2 fallback as minimum for interoperability with legacy systems. This strategy will ensure high level of confidentiality and integrity during the data transit.

***FTP/SFTP outdated**: SFTP builds on the outdated FTP protocol by incorporating SSH (Secure Shell) for added security. However, this introduces greater complexity in setup and configuration, making it harder to manage and maintain. While SFTP has its uses, it is increasingly regarded as outdated in modern environments due to the availability of cloud storage, newer protocols with enhanced security, and the demand for scalability and user-friendly solutions. Modern tools, such as cloud storage platforms, APIs, and other flexible protocols, offer advanced features and superior performance compared to SFTP. This protocol is not really recommended to ensure real-time data reporting and exchange.

2.3 Data Processing and Analytics

The IOTC VMS Pilot Project requires efficient and accurate data processing to ensure the reliability and usability of transmitted information. Therefore, the IOTC Pilot system shall include:

- **Data Validation.**
- **Analytics and Event Processing.**

2.3.1 Data Validation

Data validation is critical to ensuring the reliability and integrity of information processed by the IOTC VMS Pilot System. The validation framework includes:

- **Automated Integrity Checks**:
  - Positional data validation:
    - Latitude between - 90° and + 90°.
    - Longitude between – 180° and + 180°.
    - Speed within 0-100 knots.
    - Course within 0° - 360°.
  - Verification that all mandatory fields (e.g. timestamp, vessel ID…) are present, consistent and correctly formatted.

- **Anomaly Detection**:
  - Duplicate detection: identification of duplicate records to prevent redundancy in reporting and processing.
  - Unknown vessel data: Automatic flagging when positional data is received from vessels not registered in the system database.
  - Detection and flagging of incomplete or inconsistent data points (**e.g. timestamp, vessel ID, geolocation fields…**) or incorrect formats.

2.3.2 Analytics and Event Processing

The IOTC VMS Pilot System shall integrate robust analytics and event processing capabilities to ensure effective monitoring and actionable insights. The framework includes the following features:

- **User/Operator Alerts**:
  - MTU Technical alarm (**Power Up/Down, GNSS Signal Lost, Antenna Blockage/obstructed, Tampering/intrusion detection**).
  - Geofencing Alerts (**Entering/Exiting Area, InZone, Speed in Zone, Proximity to selected Area**).
  - Position Report Overdue & Report too often Alerts.

- **System Alerts**:
    - Unknown reporting Vessel
    - Data Consistency Alert: **Based on Data Validation section above**, inconsistent data will be flagged and alerts triggered.
    - VMS data Distribution to external system crashed down Alert: Alert to monitor the VMS data distribution and exchange in both ways with third systems.
- **Alerts settings**:
    - Alerts can be shared with other users/operators.
    - Alerts can be classified by level of severity (Emergency, only for guidance…).
    - Alerts can be configured according to seasonality period (active/inactive periods).
    - Alert triggered can be notified by email to recipients with possibility to add a message in the notification.
- **Reporting and Visualization**:
    - All Alerts raised shall be visualized in a Dashboard from where the operator will consult and treat these alerts with possibility to close it afterwards.
    - Alerts Reports features shall be available together with Export possibilities (e.g. Excel) for operational reviews.

2.4 User Interface

The IOTC VMS Pilot Project's user interface is designed to provide intuitive tools for real-time monitoring, vessel tracking, and geographic data management. This section details the minimum features requirements the system should have.

2.4.1 General Principles

To support the diverse needs of stakeholders in the IOTC VMS Pilot Project, the User Interface should bring simplicity and flexibility in the day-to-day monitoring hence the principles below:

- The interface emphasizes simplicity and usability to accommodate diverse user groups.
- Supports role-based customization to align with the operational needs of different stakeholders.

- Responsive design feature, ensuring compatibility with mobile and desktop platforms.
- Provides clear and interactive tools for visualization of vessel data and effective decision-making.

2.4.2 Display and Mapping Tools

The display and mapping tools of the IOTC VMS Pilot Project interface focus on delivering clear, actionable visualizations. These tools allow operators to efficiently monitor vessel activities and analyze spatial data.

- **VMS Data Visualization:**
  - Display of vessel trajectories for real-time monitoring and historical analysis.
  - Display last positional data as icons on navigational charts.
  - Display vessel labels together with the positional data.
  - Display trajectories with color-coding based on speed.
  - Arrow indicators to highlight direction and movement trends.
- **Basic Features:**
  - Include options to zoom in/out and pan across charts.
  - Drawing tools directly available from the map for Geographical Objects (zone/ annotations) creation.
  - Measurement tool to calculate distances on the map.
  - Enable a Full screen option for the map display
  - Support simultaneous display of map windows to support comparative analysis.
- **Advanced Features:**
  - **Distance Measurement**:
    - Draw and calculate segment lengths, directions, and bearings directly on the map.
  - **ETA Calculation**:
    - Estimate arrival times based on vessel positions, speed, and course drawn on the map.
  - **Tracking Replay**:
    - Replay vessel trajectories for historical analysis and compliance reviews.
  - **Mobile Density Maps (heatmaps)**:

- Dynamic clustering of vessel icons for improved visualization at different zoom levels
- Visualize vessel densities filtered by fleet, date, or geographic zone.

2.4.3 Customization and Filtering

Customization and filtering options enable users to tailor the interface to their specific operational needs, ensuring they can focus on the most relevant data for decision-making in the context of the IOTC VMS Pilot Project.

- **Custom Views:**
  - Allow operators to customize chart displays by selecting zones, trajectories, positional data, and annotations (landmarks).
  - Include customizable trajectory visualization, enabling users to focus on specific vessels or fleets.
  - Display customization of Geographic Objects:
    - Icon shape, size, and color.
    - Line style and color.
    - Fill color and opacity.
  - Vessel Icon: Configurable vessel icons according to vessel type, group of vessels, vessel status (**e.g. Stationary, MTU tampered, active/unactive**).
- **Filtering Options:**
  - Filter vessel positions using criteria such as:
    - Date ranges (**e.g., last X days, between two dates**).
    - Fleet or group of vessels.
    - Vessel speed.
    - Zones.

2.4.4 Map and Layer Management

These specifications below are the minimum requirements needed for monitoring Vessel activities within the IOTC area of competence.

- **Standard and coverage:**
  - Display data marine charts (e.g. C-map) covering waters under IOTC governance.

- Comply with **WGS84** geodetic standards for positional accuracy.
- Base maps with resolutions ranging from **1:500,000 to 1:3,500,000** for global and regional overviews.
- Incorporate additional layers like Open Street map and Google maps.
- Include layers for day/night limits, date and time and graticule grids (manual or automatic).

- **Geographical Objects (GO) Management**
  - Create and manage geographical objects interactively:
    - Drawing directly on the map using Line, Circle and polygons tools.
    - Entering positions and parameters directly in a management interface.
    - Importing predefined geographic areas in formats such as **Shapefiles**
  - Integrate **GO** with Alerts to monitor vessel movements and compliance.
  - Enable operators to share the GO creation with other Users.

2.4.5 Remote Access to Web Interface

The Remote Web Interface shall support real-time and secure access to the VMS Pilot system for stakeholders, enabling concurrent access, seamless monitoring, data analysis and decision-making from any location.

- **Secure Web Access**:
  - **The web interface** will use HTTPS for secure access to the VMS system.
  - **Authentication mechanism** (Login/password as a minimum) to be provided by the VMS Pilot Platform to authenticate users and preserve Data confidentiality.
  - **Automatic logout and Password change** requirements after a certain period of time shall be mandatory to enhance Data security access.
  - **Access Monitoring**:
    - Record of all log in /log out.
    - Login Attempt audit report (successful and unsuccessful).
  - **IP Restrictions / SSL certificate**: The system IT network shall have the possibility to limit access to predefined IP ranges for enhanced security (**Firewall configuration**).

- **Cross-Platform Compatibility**:
  - The system will provide a fully responsive design web-based interface to support seamless access via desktop and mobile devices.
  - Compatible with modern web browsers, including **Google Chrome**, **Mozilla Firefox**, and **Microsoft Edge**.
  - Supports concurrent access by multiple users, ensuring real-time updates and operational consistency.

- **Multi-Role Support:**
  - Permissions based on user roles, including as a minimum administrator, operator, and viewer roles.

2.5 VMS Data Distribution

Efficient and secure data distribution ensures timely delivery of VMS information to the IOTC Secretariat, Volunteer CPCs, and other authorized stakeholders. This framework supports real-time VMS data exchange, secure transmission and data customization.

2.5.1 Key Distribution mechanisms

The System shall allow below features and possibility to ensure proper VMS data Distribution.

- **APIs**: RESTful APIs and SOAP v1.2 with Two-Way SSL for ensuring Real-time data exchange with external systems like FMCs and RFMOs, supporting JSON and XML formats for interoperability.
- **Secure Communication Protocols**: HTTPS, HTTPS POST, or HTTPS GET for secure and real-time / near real-time VMS data transmission and exchange.
- **Standardized Data formats:** NAF/XML/FLUX P 1007/JSON/CSV.

2.5.2 Data Customization

- **Role-Based Filtering**: Tailored data for stakeholders (**e.g., flag, port, coastal States, CPC, RFMO…**). Possibility to filter the data fields to be exchanged.
- **Spatial/Temporal Filters**: Customizable by geographic zones (**e.g., EEZs**) and timeframes.
- **Vessels/Fleet Filtering**: Filter vessel or group of vessels to be considered for the VMS data exchange.

2.5.3 Security Measures

- **Encryption**: TLS 1.3 for all transmissions; TLS 1.2 fallback for legacy systems.
- **Audit Trails**: Logging of all data deliveries for accountability.

2.6 Technical Specifications

2.6.1 System Architecture

To meet the operational requirements of the pilot project, the system architecture must adopt modern, flexible solutions that ensure efficient implementation and simplified maintenance. Consequently, a cloud-based solution is highly recommended to optimize initial and operational costs, enhance feasibility, and simplify deployment.

The proposed cloud-based architecture for the VMS system will provide scalability, resilience, security, and operational efficiency. A leading cloud service provider (**AWS, Azure, or GCP**) should be selected to leverage global infrastructure, including multi-region and multi-zone deployment, ensuring redundancy, low latency, and high availability. The cloud environment should incorporate virtualization and containerization (e.g., Docker/Kubernetes) to enable efficient resource allocation, dynamic scaling, and streamlined management.

In the cloud-based environment, automated backups and disaster recovery plans are included to ensure real-time data replication to secondary regions, regular snapshots, and robust testing to guarantee data protection and rapid recovery in case of failures. Additionally, Cloud environment from leading providers offer security measures such as data encryption (**in transit**), role-based access control, cloud-native firewalls, and adherence to international compliance standards (e.g., ISO 27001, GDPR).

Furthermore, redundancy will be achieved through multi-zone deployments, failover mechanisms for critical components, and high-availability database clusters. Monitoring and logging systems continuously track performance and security, providing actionable insights to maintain operational integrity. This modern, scalable architecture ensures a secure and efficient foundation for the IOTC VMS system.

2.6.2 Performance Standards

The performance standards defined for the VMS system ensure its ability to handle substantial workloads while maintaining fast and reliable data transmission.

- **Transactions:** The system must handle a minimum of **5 transactions per seconds** of **50 transactions per minute** and **100,000 transactions per day** to meet operational demands. Simultaneously, the system's ability to support a large number of concurrent users is critical for overall efficiency.
- **User Load:** The system should be capable of supporting up to **100 concurrent users** without performance degradation. To complement these requirements, latency must remain within acceptable limits, even during peak usage.
- **Latency:** Data transmission delays must be kept under **5 minutes**, ensuring sufficient responsiveness for real-time operations.

2.6.3 Database capacity

Database capacity is a key element of the system, ensuring the efficient management of vessel data during the pilot phase and beyond.

- **Storage Capacity:** The database must support storing of all required information for at least **1000 vessels** during the Pilot Project phase. Scalability is essential to support the project's future operational needs.
- **Scalability:** The system must be designed to accommodate **10 times more vessels or data domains** to meet the demands of the operational phase after the pilot.
- **Data Archiving:** Data retention and archiving also play a crucial role in ensuring compliance and maintaining historical records. In the frame of this Pilot project, a recommendation is given for a minimum retention period of **5 years**.

D. Recommendations of Standard Operating Procedures

I. Introduction

These Standard Operating Procedures (SOPs) are recommendations for providing step-by-step instructions for implementing and managing the IOTC VMS Pilot Project. It aligns with relevant IOTC Resolutions, including **Resolution 12/02** on data confidentiality and **Resolution 15/03** on Vessel Monitoring System (**VMS**) operations.

These SOPs should be designed to propose a framework for the launch of this Pilot Project and guidelines along with this project. However, these SOPs shall at the same time provide flexibility and area for improvements, especially regarding below aspects:

- Extension of vessel target according to Amendments of Res 15/03 (**ref IOTC-2023-VMSWG06-03**)
- Expansion of the Volunteer CPCs Panel: Broader participation will strengthen the project's data baseline, user feedback, facilitate effective evaluation, and lay the foundation for a potential **IOTC Regional VMS**.

II. Objectives of IOTC VMS Pilot Project SOPs

The **Standard Operating Procedures (SOPs)** for the IOTC VMS Pilot Project aim to establish clear guidelines and processes to ensure the successful implementation, management, and evaluation of the pilot project. The following objectives have been identified to support the broader goals of effective **Monitoring, Control, and Surveillance (MCS)** of fishing activities in the IOTC are of competence:

- **Ensure Compliance with IOTC Resolution**:
    - Align with **Resolution 12/02** (data confidentiality) and **Resolution 15/03** (VMS requirements).
- **Standardize VMS Processes:**
    - Streamline data collection, reporting, and management for consistent and reliable operations across participating CPCs.
- **Establish Clear Governance**:
    - Define roles for the IOTC Secretariat, CPCs, and vessel operators, ensuring effective oversight and accountability.

- **Support Scalability:**
  - Allow for future **expansion** of vessel coverage and broader participation of volunteer CPCs.

- **Strengthen Information Sharing and Data Security:**
  - Implement an **Information Sharing Agreement** to govern VMS data access, ensuring data confidentiality, secure transmission, and controlled dissemination among Volunteer CPCs and the IOTC Secretariat.
  - Protect data integrity and availability through robust access controls and security protocols.

- **Enhance Monitoring, Control, and Surveillance (MCS):**
  - Use shared VMS data to support evidence-based fisheries management, policy updates, and scientific research.

- **Promote Continuous Improvement:**
  - Facilitate stakeholder feedback and regular updates to SOPs to adapt to evolving needs and technologies.

III. Stakeholders, Roles and Responsibilities

The stakeholders for this pilot project are identified as follows:

- **IOTC Secretariat**
  - **Project Oversight**: Coordinate and manage the VMS Pilot Project implementation.
  - **Data Management**: Collect, process, and securely store VMS data while ensuring compliance with Resolution 12/02 on confidentiality.
  - **Information Sharing**: Administer the Information Sharing Agreement to regulate access, dissemination, and usage of VMS data among stakeholders.
  - **Reporting**: Prepare regular compliance reports, performance evaluations, and recommendations for the VMS Working Group and Commission.
  - **Support**: Provide technical guidance to Volunteer CPCs and vessel operators for troubleshooting and VMS compliance.
- **Volunteer CPCs:**
  - **Implementation**: Ensure vessels flying their flag comply with VMS requirements **Res 15/03**, including timely and accurate data transmission.

- **Compliance**: Monitor VMS operations, address technical failures, and enforce reporting requirements in line with Resolution **15/03**.
- **Feedback**: Provide feedback on VMS performance, challenges, and improvements to the VMS Working Group and IOTC Secretariat.
- **Collaboration**: Support regional cooperation through active participation and data sharing as outlined in the **Information Sharing Agreement**.

- **Mobile Communication Service Provider (MCSPs):**
  - **VMS Data Transmission**: According to Option 3 "Partially Centralized", ensure real-time, reliable and secure transmission of VMS data from vessels to IOTC VMS Pilot Platform.
  - **Technical Support**: Assist with troubleshooting connectivity issues, equipment malfunctions, and data delivery failures.
  - **Compliance**: Ensure VMS Data delivery meets technical specifications and security requirements outlined in the project framework.

- **Vessel Operators:**
  - **VMS Device Management**: Ensure VMS devices remain operational, tamper-resistant, and unobstructed at all times.
  - **Manual Reporting in case of MTU Communication breakdown**: Submit positional data every **4 hours** to the Volunteer Flag State FMC in case of VMS device failure.
  - **Compliance**: Follow reporting requirements and cooperate with Volunteer Flag CPC, MCSP, and VMS Pilot Platform technical partners for VMS performance.
  - **Alerts and Notifications**: Immediately report any VMS malfunction or suspicious activity to the Volunteer Flag State FMC.

- **VMS Working Group:**
  - **Project Monitoring**: Oversee the progress, implementation, and evaluation of the VMS Pilot Project.
  - **Policy Recommendations**: Review feedback and propose amendments to VMS operational processes, including extensions to vessel targets and updates to Resolution 15/03.
  - **Stakeholder Coordination**: Facilitate discussions between the IOTC Secretariat, Volunteer CPCs, and technical partner to resolve issues and identify improvements.

- **Technical Oversight**: Provide expertise on data security, confidentiality, and technical implementation.

- **Technical Partner:**
  - **System Development and Support**: Implement, configure, and maintain VMS software, ensuring compatibility with data transmission requirements.
  - **Troubleshooting**: Provide technical assistance to resolve hardware, software, or data processing issues.
  - **Training**: Train stakeholders like Volunteer CPCs and the IOTC Secretariat on VMS software usage and system maintenance.
  - **Scalability**: Support future expansions, such as additional vessel categories and regional integration (**integration of new Volunteer CPCs**).

IV. Operational Processes

1. Data Collection and Transmission

We can split the Dataset into two categories, the **Dynamic Positioning Data and Non-Dynamic Data** or in other words Declarative Data. Collection of this information can be done in different ways.

1.1 Dynamic Positioning Data

The **IOTC Resolution 15/03** shall be the framework for the Vessel target, VMS data, reporting frequency and Manual reporting. and possibly adjusted by related amendments during the Pilot Project phase. Moreover, the related amendments proposed to that resolution should be considered as possible enhancements and improvements and depending on the willingness of the Volunteer CPCs. Below table resume scope and requirements.

Scope	Resolution 15/03	Res 15/03 Amendments (Proposed)
Vessel Target Criteria	Vessels ≥24 meters or vessels operating outside their Flag State EEZ	Expanded to include vessels ≥12 meters in length overall
Vessel Identification	Unique vessel ID (e.g., RCS, IMO number, registration)	idem

Geographical Position	Latitude and Longitude with error < 500m, 99% confidence	Increased accuracy: Error < 50m, 99% confidence
Date and Time	UTC-based timestamp of position report	idem
Speed	Not required	Speed of the vessel (in knots)
Course	Not required	Course (direction of travel)
Reporting Frequency	Every 4 hours	Reduced to every 2 hours (near real-time)
Automatic Geofencing Reports	Not required	Proposed: Entry/exit notifications for designated zones transmitted by the MTU if it enables to do so (EEZs, restricted areas).
Tampering Alerts	Optional if MTU is equipped with such mechanism	idem
Event Generated Report	Not required	Proposed: -Power Up/Down Msg -Antenna obstructed (If MTU enables such feature)
Manual Reporting in case of MTU Communication breakdown	Required every 4 hours if VMS fails	idem
Polling Feature (only for option 3 Partially Centralized	Not required	Proposed: Possibility to test the Polling feature*

Table 3: IOTC Resolution 15/03 and its proposed amendments breakdown.

**One CPC suggested to remove this feature.*

The Transmission of this information should be done real-time and/or near-real-time under two different reporting methods:

- Option 2 "Shared Decentralized". Volunteer CPC opting for that method: **to be confirmed**
- Option 3 "Partially Centralized". Volunteer CPC opting for that method: AUSTRALIA

For both reporting methods, data format and communication protocols are defined in the technical section (refers to C. Design of the IOTC Pilot Project on VMS).

1.2 Non-Dynamic Data

This data type is Declarative data that is filled in into the System Database. An exhaustive presentation of this dataset is available in this report ***section C. 2.2.2 Declarative Data.***

This information is a combination of the IOTC RAV file + additional dataset proposal. In the frame of this Pilot Project, in the first steps of the implementation process, decisions will be taken on the scope of non-dynamic data to be considered during this project.

As per the data transmission and population, there are many options to explore:

- **Automatic Import**: The RAV information could be imported into the VMS System Database. This import feature could be realized to populate the System Database during what we can name the database migration. This could be done once a while but does not constitute a proper database synchronization on a routine basis.
- **Manual data input**: For new dataset coming from new vessels (expansion of RAV list) or added to existing vessel registry (RAV file):
    - Vessel operators or Volunteer CPCs fill in a form (can be online) and transmit it to IOTC Secretariat. Data is then filled in into System Database by the IOTC Secretariat afterwards.
    - Volunteer CPCs can have remote access to the System User Interface to fill in the dataset directly into the System Database. This method is easier, more reliable and will increase data consistency and efficiency. This remote access will be done based on role-based permissions to ensure data security and confidentiality.
- **Database Synchronization**: Databases Synchronization between Volunteer CPCs and IOTC VMS Pilot System Database. This option is more costly and complex and may face technical limitations, especially with legacy systems but it will ensure data quality and reliability, automatic database update and information unicity by pushing aside human mistakes.

2. Testing Technical Scenarios

Technical scenarios will be tested to assess the reliability, security, and functionality of the IOTC VMS Pilot Project under various conditions.

2.1 Objectives

- Verify data accuracy, reporting frequencies, and real-time transmission capabilities.
- Test different reporting methods and the different Scenarios.
- Validate compliance with Resolution 15/03 and proposed amendments.

2.2 Key Test Scenarios

- **System Integration Tests:**
  - Validate compatibility between Volunteer CPCs FMC systems and the centralized VMS platform.
  - Simulate data transmission under both decentralized (Option 2) and partially centralized (Option 3) models.
- **Communication Breakdown:**
  - Test manual reporting mechanisms when vessel VMS devices fail.
  - Assess response time and notification procedures for technical issues.
- **Geofencing and Alerts:**
  - Evaluate entry/exit notifications for designated zones (e.g., EEZs, restricted areas).
  - Test tampering alerts and event-triggered reports (e.g., antenna obstructions).
- **Polling Feature:**
  - Under Reporting method option 3, conduct pilot tests for polling functionality to request positional data on demand.
- **Data sharing Protocol:**

- Test VMS data access and sharing according to the Information Sharing Agreement developed and proposed in **D. V. Data Governance and Safeguards**.
- Emergency reporting: Simulate search and rescue scenario requiring immediate data access.

3. Training and Capacity Building

Effective training and capacity-building efforts are essential for the successful implementation of the VMS Pilot Project, ensuring all stakeholders understand their roles and responsibilities. Targeted training will mitigate risks such as technical failures, inconsistent reporting, and data security breaches. Tailored programs will address the needs of:

- IOTC Secretariat & Technical Support Team (**Administrator Role**)
- VMS operators (**Operator Role**)
- Volunteer CPCs. (**Viewer Role**)

These efforts aim to equip stakeholders with the tools and knowledge to operate the VMS system efficiently, adhere to protocols, and maintain data governance consistency across the region.

3.1 Training Components

- **General System training**:
  - General Overview of the System Components.
  - DataFlow.
  - Data sharing Protocol.
  - **Applies to**: IOTC Secretariat/VMS Operator/Technical Support Team/Volunteer CPC/IOTC VMS Working Group.
- **Technical / Administrator Training**:
  - Technical support.
  - Initial set-up and Configuration.
  - Data Distribution connection and settings.
  - Role-based account Creation and management.
  - User role-based permissions.
  - Troubleshooting.

- **Applies to**: IOTC Secretariat and Technical Support Team.

- **User Training**:
  - IOTC VMS Software usage for day-to-day operation.
  - User Interface features.
  - Software features and functionalities.
  - Introduction to reporting procedures and compliance with SOPs.
  - Manual Reporting protocol during MTU Communication breakdown.
  - **Applies to**: VMS Operator/Technical Support Team/Volunteer CPC*.

To be defined by IOTC Secretariat whether the Volunteer CPCs will follow this training session or if lighter training course (for Viewers Only) will be designed for this stakeholder.

3.2 Delivery Methods

These training courses can be delivered either by:

- Online webinars and Tutorials (**For Viewer only role**).
- In-person workshops and hands-on sessions (**For Administrator /Operator**).
- Online sessions (**For Operator / Viewer Only**).

3.3 Training Materials

Training materials will be provided in French and English and include:

- User manuals and quick-start guides.
- Technical and Troubleshooting references.
- FAQ documents.
- Training presentations (ppt) / Cases Studies.

3.4 Post Training evaluation

Post-training evaluations are essential to assess participant knowledge and readiness, ensuring they have fully understood the training material and can apply it effectively. These evaluations help identify gaps in understanding and areas requiring further attention. To support continuous improvement, ongoing refresher sessions should be provided as needed, reinforcing key concepts and addressing emerging

challenges. Feedback forms and evaluation documents should be used to collect participant input on the training sessions, offering valuable insights to refine and enhance future training programs. This iterative approach ensures sustained learning and optimal performance across all stakeholders.

V. Data Governance and Safeguards

Data governance and safeguards are critical components of the IOTC Pilot Project on VMS, ensuring that data is managed responsibly, securely, and in compliance with relevant regulations. IOTC Commission will rely on its existing resolutions that rule and organize data sharing and dissemination like the IOTC **Resolution 15/03**, its amendments and the **Resolution 12/02**. The IOTC Commission could also benefit from additional frameworks like the **Information Security Management System (ISMS) international standards** as outlined in **ISO/IEC 27001** and **ISO/IEC 27002**.

This section outlines the principles, policies, and technical measures required to achieve robust data governance.

1. Overview of ISMS Standards (ISO/IEC 27001 and ISO/IEC 27002)

The **ISO/IEC 27001** and **ISO/IEC 27002** standards provide a comprehensive framework for managing information security. These standards focus on safeguarding the confidentiality, integrity, and availability of information assets through systematic processes, policies, and controls.

- **ISO/IEC 27001**: Defines the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (**ISMS**). It emphasizes a risk-based approach to identify and mitigate information security risks.
    - Establishment of a risk management process to identify, assess, and treat information security risks.
    - Development of a robust policy framework for information security aligned with organizational goals.
    - Implementation of controls to ensure the protection of critical data assets.
    - Regular audits and continual improvement of the ISMS to adapt to new challenges.

- **ISO/IEC 27002**: Offers practical guidelines and best practices for implementing the controls outlined in ISO/IEC 27001, focusing on:
    - **Access Control**: Ensuring that only authorized personnel can access sensitive information.
    - **Incident Management**: Procedures to detect, respond to, and recover from security breaches.
    - **Encryption**: Using encryption to protect data in transit.
    - **Business Continuity**: Establishing and maintaining measures to ensure critical functions can continue during and after disruptive incidents.
    - **Supplier Relationships**: Managing third-party risks to ensure compliance with information security policies.

The IOTC Secretariat and the VMS Working Group could explore the above possibilities to reinforce the IOTC Data policy.

2. Data Governance Principles

The data governance framework for the IOTC Pilot Project should be designed to:

- **Ensure transparency** in data collection, storage, and processing, as mandated by IOTC Resolution 15/03 and its amendments.
- **Promote accountability** among stakeholders.
- **Maintain data quality**, consistency, and integrity.
- **Uphold confidentiality and data privacy** in compliance with IOTC Resolution 15/03 and 12/02.

3. Information Sharing Agreement

An Information Sharing Agreement (**ISA**) will be developed and signed by Volunteer CPCs that want to participate to this data sharing and the IOTC Secretariat. The ISA establishes a structured framework for secure, controlled, and transparent data exchange. Key components of the ISA include:

- **Scope of Shared Data:**
    - **Dynamic Positioning Data**: VMS data (**latitude, longitude, speed, course…**) as outlined in Resolution 15/03 and its proposed amendments.
    - **Vessel targets**: According to IOTC RESOLUTION 15/03 and its proposed amendments.

- Data must be transmitted by Flag CPCs when vessels operate within the IOTC Area of Competence.
- VMS data must be transmitted in real-time and/or near-real time to the IOTC VMS Pilot Platform.

- **Authorized Recipients:** List of authorized users, their roles, and access privileges.
  - **Flag CPC Designated Authorities**: Retains ownership of VMS data and has automatic access to their own flagged vessels' data without formal requests, as outlined in Resolution 15/03 and its related amendments.
  - **IOTC Secretariat**: Authorized staff responsible for centralized data management, processing CPCs' VMS Data requests, and monitoring.
  - **Coastal CPCs**: Limited access to VMS data for flagged vessels entering their EEZ, as outlined in the amendments to Resolution 15/03.
  - **Requesting CPC**: Authorized to access data prior written authorization of Flag State CPC or under purposes as outlined in Paragraphs 16a and 16b.

3.1 Data sharing Protocol

VMS data will be shared upon CPC Request for having access to VMS Data. Below Sharing protocol is structured to balance operational efficiency, security, and data confidentiality. This Sharing protocol distinguishes between requests that do not require prior approval from the Flag CPC and those that explicitly require it, ensuring clarity and alignment with Resolution 15/03 proposed amendments.

- **Requests Not Requiring Flag CPC Approval:**
  - **Search and Rescue Operations (SAR)**: VMS data can be accessed directly by a requesting CPC for emergencies, such as search and rescue operations, under predefined conditions. The IOTC Secretariat will inform the Flag CPC after the data is shared.
  - **Planned Surveillance**: A requesting CPC may access data for active surveillance planning operations. For this purpose, the geographic area of the planned surveillance activity shall be provided to the IOTC Secretariat.
  - **Active Surveillance Operations**: VMS data is provided for detecting vessels during surveillance and for vessels operating within a 100 nautical mile radius of the surveillance area, up to 10 days prior to the operation.
  - **Coastal CPC Access**: Automatic access to positional data for flagged vessels entering their EEZ.

- **Requests Requiring Prior Flag CPC Approval:**

- **CPCs Data Requests**: Requests for VMS data for purposes other than the one listed in Resolution 15/03 proposed amendments Paragraph 16 require explicit Flag CPC approval.
- **Third-Party Access**: Sharing VMS data with any entity other than authorized recipients must be approved by the Flag CPC.
- **IOTC Scientific Committee Data Requests**: Requests for scientific analysis or other extended uses not explicitly covered under this Agreement require prior Flag CPC consent.

4. Data Policy

Data policy defines the rules, standards, and procedures for management, access, retention, and security of data within the IOTC Pilot Project on VMS. It ensures that data is handled responsibly, transparently, and in alignment with organizational objectives and compliance requirements. This section provides a structured framework to guide how data is accessed, stored, and shared.

4.1 Data Access and Permissions

The Data Access and Permissions should be linked to the Data sharing Protocols rules and procedures which were built based on a strict application of IOTC Resolution 15/03 and its proposed amendments. Its usage must be limited solely for compliance monitoring as well as for scientific assessments and management decisions within IOTC Mandates. Data access must be done using secure dissemination mechanisms as described in the technical design proposal in **C. Technical Design**.

Data Access could also be done through the remote access to the VMS System User Interface. Based on **role and access right restrictions**, stakeholders like Volunteer CPC and more generally Requesting CPC could have access to the VMS data by visualizing it directly from the VMS pilot Platform. These limitations and right restrictions should be implemented for the following criteria:

- By vessel, fleet, CPC Flag
- By area (**EEZ, specific zone**)
- By time range

Once authorized recipients approved and constituted, IP restriction mechanism could also be implemented to restrict access only to a specific IP list.

According to the ISA, the user account can also be limited in time by implementing an expiry date.

4.2 Data retention schedule

Data should be retained for at least the entire duration of the IOTC VMS Pilot Project unless extended retention is required by applicable laws or agreements. To ensure continuity of the project and prepare for the operational phase, the following aspects will be followed:

- **Minimum Data Storage Duration:** 2 years, ensuring that essential project data remains accessible during its critical evaluation and implementation phases.
- **Maximum Data Storage Duration:** 5 years, to accommodate extended analyses, legal compliance, and long-term planning needs.
- **Secure Storage:** Data will be stored with redundancy mechanisms to prevent loss and ensure availability in case of system failures. Disaster recovery measures will be in place to enable rapid restoration of operations.
- **Secure Destruction Mechanism:** When data is no longer needed, it will be securely destroyed using industry-standard methods to ensure that sensitive information is permanently erased and cannot be recovered.

4.3 Data Security and Confidentiality

The IOTC Secretariat should implement rules and procedures to prevent unauthorized data dissemination, mitigate data security breaches and keep continuous monitoring of access and usage. Below are some recommended leads that could be explored:

- **Legal Safeguards**: Implementation of **Memoranda of Understanding (MOUs)** and binding legal agreements like **Non-Disclosure-Agreement** (**NDA**) ensuring data confidentiality and proper use.
- **Physical Safeguards**: Secure hosting environments with redundancy and disaster recovery plans to be proposed by the Cloud Services Provider.

- **Secure Data Transmission**: Encrypted channels and robust authentication protocols for all data exchanges.
- **Audit Logs**: Continuous monitoring of access and usage to ensure compliance with ISA guidelines.
- **Emergency Destruction**: Data provided for surveillance purposes must be deleted after specified timeframes (72 hours post-operation, per Paragraph 19).

- **Training:** All personnel involved in the project will undergo training on data governance and security best practices

Periodic reviews of the data governance framework and safeguards will be conducted to ensure they remain aligned with evolving requirements, best practices, and the objectives of the IOTC Pilot Project. These reviews will enable the identification of areas for improvement and ensure the framework's continued effectiveness.

Additionally, mechanisms should be implemented to gather feedback from Volunteer CPCs and other stakeholders on the performance and applicability of data governance measures. This feedback loop will provide valuable insights to refine and adapt the governance framework to meet stakeholder expectations and project needs.

VI. Monitoring and Validation

The project's success relies on a robust monitoring and validation framework encompassing three key areas:

- **Performance Monitoring:**
  Key performance indicators (**KPIs**) include data reporting accuracy, system uptime, and user compliance rates. Regular performance reports will be submitted to the IOTC VMS Working Group for review.

- **Validation Processes:**
  Data quality checks and system validation, including periodic testing and scenario simulations, will ensure data accuracy, system integrity, and reliability under various conditions.

- **Continuous Improvement:**
  Stakeholder feedback will guide updates to SOPs and system enhancements. A final evaluation report will summarize successes, challenges, and recommendations for scaling the pilot project.

This framework ensures the project meets its objectives while adapting to future needs.

E. Conclusion

The IOTC VMS Pilot Project represents a critical step toward enhancing regional fisheries governance and combating IUU fishing in the Indian Ocean. By leveraging innovative vessel monitoring technologies and harmonized data-sharing protocols, the pilot aims to address current challenges while establishing a scalable framework for a future regional VMS system. Through robust stakeholder collaboration, technical testing, and adherence to international standards, the initiative seeks to foster transparency, improve compliance, and strengthen regional cooperation. As said previously, the outcomes of this project will provide a solid foundation for sustainable fisheries management, setting a precedent for regional monitoring efforts globally.

F. Appendix a -List of figures and tables

List of Figures

List of tables

G. Appendix b-List of acronyms

Acronym	Meaning
AOI	Area of Interest
API	Application Programming Interface
AWS	Amazon Web Services
CMM	Conservation and Management Measures
CPC	Contracting Parties and Cooperating Non-Contracting Parties
EEZ	Exclusive Economic Zone
FLUX	Fisheries Language for Universal Exchange
FMC	Fisheries Monitoring Center
GCP	Google Cloud Platform
GO	Geographical Object
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IOTC	Indian Ocean Tuna Commission
ISA	Information Sharing Agreement
IS	Information System
ISMS	Information Security Management System
IUU	Illegal, Unreported, and Unregulated (Fishing)
JSON	JavaScript Object Notation
KPIs	Key Performance Indicators
LES	Land Earth Station
LOA	Length Overall
MCSP	Mobile Communication Service Provider
MCS	Monitoring, Control, and Surveillance
MtoM	Machine-to-Machine
MTU	Mobile Transmitting Unit
NAF	North Atlantic Format
RAV	Record of Authorized Vessels
RESTful API	Representational State Transfer Application Programming Interface
RFMO	Regional Fisheries Management Organization
SOAP	Simple Object Access Protocol
SCS	Satellite Communication Systems
SOP	Standard Operating Procedure
SPRFMO	South Pacific Regional Fisheries Management Organization
SFTP	Secure File Transfer Protocol

SSL	Secure Sockets Layer
TLS 1.2	Transport Layer Security version 1.2
UTC	Coordinated Universal Time
VMS	Vessel Monitoring System
WCPFC	Western and Central Pacific Fisheries Commission
XML	eXtensible Markup Language
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business

H. Appendix c- CPCs VMS Overview

Country	VMS Adoption for >=24m and <24m High Seas	Total Vessels on IOTC Record	Vessels >=24m	Vessels <24m Operating Outside EEZ	>=24m with Satellite VMS	<24m with Satellite VMS	FMC Exists	FMC with Hardware/Software for Automation	Type of VMS	VMS Transmits	Transmission Intervals (hours)	Technical Failure Reporting (hours)	Failure Reporting Method
Australia	Yes	49	12	37	12	37	Yes	Yes	Iridium, Orbcomm	ID, Location, Time	1	24	Email
China	Yes	97	97	0	97	0	Yes	Yes	Inmarsat, Argos	ID, Location, Time	1	1	Email
European Union	Yes	119	98	21	98	19	Yes	Yes	Inmarsat, Iridium, M2M, IDP (Orbcomm)	ID, Location, Time	1	4	Email
Indonesia	Yes	567	448	64	448	64	Yes	Yes	Inmarsat, Argos, Iridium, Orbcomm, Global Star	ID, Location, Time	1	1	n.c.
India	Yes	4	4	0	0	0	Yes	Yes	N/A	ID, Location, Time	24	24	radio
Iran	Yes	1312	573	739	34	44	Yes	Yes	Thuraya	ID, Location, Time	1	0	none
Japan	Yes	166	166	0	166	0	Yes	Yes	Argos, Iridium, Inmarsat-C	ID, Location, Time	4	4	Email
Kenya	Yes	5	5	0	5	0	Yes	Yes	Iridium	ID, Location, Time	1	4	Email
Korea	Yes	77	77	0	77	0	Yes	Yes	Inmarsat D/D+	ID, Location, Time	1	2	Email
Sri Lanka	Yes	1796	4	1791	5	1791	Yes	Yes	Iridium	ID, Location, Time	6	24	radio
Madagascar	Yes	5	0	5	0	5	Yes	Yes	Inmarsat-C, Iridium, Argos	ID, Location, Time	1	4	Email
Maldives	Yes	359	358	0	258	0	Yes	Yes	Inmarsat-C	ID, Location, Time	1	6	telex
Mozambique	Yes	0	0	0	0	0	Yes	Yes	Iridium	ID, Location, Time	2	2	Email
Mauritius	Yes	19	19	0	19	0	Yes	Yes	Inmarsat-C, Iridium, Argos	ID, Location, Time	1	4	Email
Malaysia	Yes	17	17	0	17	0	Yes	Yes	Argos, Iridium, Thuraya, IsatData Pro Orbcomm,	ID, Location, Time	1	12	Email
Seychelles	Yes	81	44	37	44	37	Yes	Yes	Inmarsat-C, Argos, Iridium	ID, Location, Time	1	6	Email
Thailand	Yes	9	9	0	6	0	Yes	Yes	Inmarsat (Orbcomm),	ID, Location, Time	1	1	Email
Taiwan (China)	Yes	240	227	13	227	13	Yes	Yes	Inmarsat-C, Iridium	ID, Location, Time	1	4	Fax
Tanzania	Yes	4	4	0	4	0	Yes	Yes		ID, Location, Time	1	6	Email
South Africa	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.	n.c.

I. Appendix d-Volunteer CPCs questionnaire

IOTC REGIONAL FMC PILOT PROJECT (SURVEY)

Segment Fleet according to IOTC Res 15/03 Para 1 (vessels >= 24 m and < 24 m fishing high seas) - Onboard VMS systems				FREE COMMENTS
1.a	Who are your MTU VMS Providers?			
	Do your MTUs integrate geofencing capacity for -sending entry/exit zones message? -Changing automatically its frequency rate?	NO	YES	
		☐	☐	
	Are your VMS service Providers able to send VMS data to multiple recipients at no additional or negigible cost?			
1.b	Additionnaly to IOTC Res 15/03 Para 5, Do the MTUs rolled out in this segment Fleet having following VMS content information: - Current geographical position of the vessel (long/Lat) with a position error to be less than 50 meters at a confidence level of 99%? - Speed and course of the vessel?			
	Do the MTUs rolled out in this segment Fleet have following Event codes: - Power UP/DOWN alerts? - Antenna obstructed alert? - Entry/exit zone alert? - Automatic intrusion/tampering dectection alert?			
1.c	Do the MTUs rolled out in this segment Fleet have polling capacity?			

Segment Fleet according to IOTC-2023-vmswg07-02 Para 2 - Onboard VMS systems				FREE COMMENTS
2.a	Would the CPC you represent willing to share VMS data in the frame of this Pilot Project for this segment Fleet? (If Yes, below queston similar to above 1.a-1.b-1.c)	NO	YES	
		☐	☐	
	Who are your MTU VMS Providers?			
	What is VMS report frequency according to your national regulation for this segment fleet?			
	Do your MTUs integrate geofencing capacity for -sending entry/exit zones message? -Changing automatically its frequency rate?	NO	YES	
		☐	☐	
	Are your VMS service Providers able to send VMS data to multiple recipients at no additional or negigible cost?			
2.b	Do the MTUs rolled out in this segment Fleet having following VMS content information: - Vessel ID? - Current geographical position of the vessel (long/Lat) with a position error to be less than 50 meters at a confidence level of 99%? - Speed and course of the vessel? - Date & time (in UTC) of the fixing of the said position of the vessel?			
	Do the MTUs rolled out in this segment Fleet having following Event codes: - Power UP/DOWN alerts? - Antenna obstructed alert? - Entry/exit zones alert? - Automatic intrusion/tampering dectection alert?			
2.c	Do the MTUs rolled out in this segment Fleet have polling capacity?			

National FMC (VMS) Software System						FREE COMMENTS
3.a	Who are you Fishing Monitoring Centre (FMC) software Provider?					
	Which data streams your system is handling	VMS	Additional Data			Other Data stream?:
		☐		Catch Data (ERS)	AIS	Oceanographic Data
				☐	☐	☐
3.b	Will the CPC you represent participate to The Pilot Project under which options	Option 2 Shared Decentralised	Option 3 Partially Centralised		Both	
		☐	☐		☐	
Option 2 Shared Decentralised						
3.c	VMS Data Format supported by your FMC system	UNCEFACT -FLUX (P1000-7)	NAF	Others (e.g. .csv, .xml, JSON…)		Others (please specify):
		☐	☐	☐		
	Is your National FMC system supports following protocols for data exchange	ftp	smtp	https		Others (please specify):
				POST	GET	
		☐	☐	☐	☐	
3.d	Automatic Data exchange: Is your system able to set automatic data transfer to third system according to following criterias:	a Vessel/group of vessels	specific areas		for a defined period of time	Others (please specify):
		☐	☐		☐	
3.e	Data policy and security: In the frame of this VMS data exchange forseen, can you depict your data policy and security regarding connection with third external system for data exchange?					
	Data policy and security: Does your system fitted with any kind of data protection mechnism that prevents the unauthorized access to the data to non authorized personnel (Could you specify)					
3.d	Hardware Architecture / hosting: Is you national FMC system hosted	Into your premise	Into a third-party Cloud Provider			Others (please specify):
		☐	☐			
3.e	Support: Is your System supported with 24/7 Operational Support?	NO	YES			
		☐	☐			
3.f	Polling command: Is your FMC software able to receive polling command from third system and consecutively to transmit it to MTUs in near real-time? And to return poll response to that third system?	NO	YES			
		☐	☐			
3.g	VMS Data storage: How many years of VMS data storage your national FMC system is keeping?					
Option 3 Partially Centralised						
4.a	Do your MCSPs route the VMS data from the Satellite Constellation used to your national FMC? (meaning the VMS data goes to MCSP server before going to your system)	NO	YES			
		☐	☐			
4.b	Do your Mobile Communication Service Providers (MCSP) support following formats for the data transmission to the Regional FMC Pilot project Platform?	UNCEFACT -FLUX (P1000-7)	NAF	Others (e.g. .csv, .xml, JSON…)		Others (please specify):
		☐	☐	☐		
4.c	Do your Mobile Communication Service Providers (MCSP) support following protocols for data exchange	ftp	smtp	https		Others (please specify):
				POST	GET	
		☐	☐	☐	☐	
4.d	Automatic Data exchange: Do your MCSP able to set automatic data transfer to third system according following criterias:	a Vessel/group of vessels	specific areas		for a defined period of time	Others (please specify):
		☐	☐		☐	
4.e	Do your MCSPs have VMS storage and VMS data replay capacities?	NO	YES			
		☐	☐			
4.f	Polling command: Do you MCSPs able to receive polling command and consecutively to return polling response in near real-time?	NO	YES			
		☐	☐			
4.g	Could you provide IOTC with technical point of contact for each MCSP?					

J. Appendix e- Bibliography and information sources

Reports and studies:

- IOTC-2019-WPICMM02 VMS Study
- TOR VMSWG – IOTC-2019 CoC 16-R(E) Appendix 8
- IOTC-CoC16-R-(E)
- IOTC-2019-CoC16-05a [E]
- IOTC–2020–S24–R[E]
- IOTC–2021–VMSWG01–R[E]
- IOTC–2021–VMSWG02–R[E]
- IOTC–2021–VMSWG02–02
- IOTC–2021–VMSWG03–R[E]
- IOTC–2022–VMSWG04–02
- IOTC–2022–VMSWG04–R[E]
- IOTC–2022–VMSWG04–03
- IOTC–2022–WPICMM05–08.
- IOTC-2022-VMSWG05-03
- ISSF-2022-06-RFMO-VMS-Comparative analysis to identify best practices
- IOTC–2022–VMSWG05–R[E]
- IOTC–2022–VMSWG05–02
- IOTC-2022-VMSWG05-04
- IOTC-2023-VMSWG06-04-Rev1
- IOTC–2022–VMSWGSS01–R[E]
- IOTC–2023–WPICMM06–08
- IOTC–2023–VMSWG06–R[E]_Rev1
- IOTC–2023–VMSWG06–03
- IOTC–2023–VMSWG06–03_Rev1
- IOTC–2023–VMSWG07–03
- IOTC-2023-VMSWG07-02
- IOTC–2023–VMSWG07–R[E]
- GFCM-Centralized VMS
- Gfcm-De-Centralized

RFMO Resolutions and official documentation

- **IOTC Resolutions 15/03 and 12/02**
- **WCPFC List of approved Mobile Transceiver Units (MTU)/ Automatic Location Communication (ALC) as of 06 February 2024**

Other documentation

- **Information Security Management System (ISMS) international standards**
- **ISO 27001 and ISO 27002**