TEST PROJECT ON COOPERATION IN EXECUTION OF VARIOUS MARITIME FUNCTIONALITIES AT SUB-REGIONAL OR SEA-BASIN LEVEL IN THE FIELD OF INTEGRATED MARITIME SURVEILLANCE (CoopP)

Final Report of Work Package 2:

Use Cases and Information Services Identification

Co-Financed under the European Integrated Maritime Policy

Table of Contents

1 Executive Summary 5
2 Background 5
2.1 Assigned Tasks and Their Expected Outputs 5
2.2 Objectives 6
3 Description of Use Cases 7
3.1 High-Level Use Cases 7
3.2 High-Level Services 8
3.3 Use Cases (detailed – sectorial) 8
4 Description of Information Services 8
4.1 The process 9
4.2 Roles and Services 9
5 Purposes Related to the Information Services 10
6 Conclusions 10
7 Recommendations 11
Annexes 12
Annex I – List of Acronyms and Abbreviations 13
Annex II – Meetings Summary 15
Annex III – List of Use Cases 16
A. High-Level Use Cases, v 3.1 16
"Baseline operations" 16
"Targeted Operations" 18
"Response Operations" 20
B. Events describing "High-Level Services" 22
1. Situational awareness 22
2. Anomalies 23
3. Operational availability 24
4. Extra ordinary 24
5. Virtual interaction 25
C. List of Use Cases for baseline maritime environment 26

Use Case ID 13b 26
Use Case ID 13c 29
Use Case ID 25b 32
Use Case ID 37 36
Use Case ID 44 39
Use Case ID 57 43
Use Case ID 70 46
Use Case ID 85 50
Use Case ID 93 54
Annex IV – List of Services 56
SECTION A: Describing the process 56
1 Explanation of the template 56
1.1 List of activities 56
1.2 List of services 56
SECTION B: Services to Use Cases 57
Use Case 13b 58
List of activities 58
List of services for the activity “analyse available information” + “collect and analyse further information” 59
Use Case 13c 63
List of activities 63
List of services for the activity “analyse available information” 64
Use Case 25b 66
List of activities 66
List of services for the activity “analyse available information” 67
Use Case 44 68
List of activities 68
List of services for the activity “analyse available information” 69
Use Case 57 70
List of activities 70

List of services for the activity “Retrieve surveillance capacities” 71
Use Case 70 73
List of activities 73
List of services for the activity “analyse available information” 74
Use Case 85 76
List of activities 76
List of services for the activity “analyse available information” 77
Use Case 93 79
List of activities 79
List of services for the activity “analyse available information” 79
Annex V – List of Purposes 81
List of purposes for information sharing 81

1 Executive Summary

The purpose of this report is to serve as a basis for further work packages and to describe how monitoring of the lawful, safe and secure conduct of maritime activities is carried out on both a daily routine basis and for intervention purposes.

The presented Use Cases describe the current situation, what could go wrong, the outcome of failures and why they occur. The use cases thus serve to highlight key areas for improvement of the Common Information Sharing Environment (CISE).

The presented List of Services in constructed with three levels of service which describe how the use cases operate in an operational macro-model including roles, input, output and other characteristics. The list of services gives guidance on how to design data formats, data models and other technical design features that would improve CISE.

The List of Purposes outlines which data needs to be available to each sector for each use case via the listed services. This is useful for access right definition purposes.

When referring to data sets, the Technical Advisory Group (TAG) data matrix has been used as a reference throughout the work.

Although the work has been co-ordinated with other work packages, it may however be useful or necessary to amend or add new entries to the material as work progresses in other WPs. All amendments should be coordinated and approved for conformity purposes.

2 Background

2.1 Assigned Tasks and Their Expected Outputs

- Work Package 2 was assigned the following tasks:
- Defining and agreeing on a selection of use cases for further analysis. All use cases together shall cover all participating sea-basins and user communities. It is suggested to identify the maximum number of use cases (even if incompletely described) to be able to agree on the ones selected for further analysis.
- Identifying common basic information services supporting the selected use cases;
- Identifying information services characteristics (business rules) and parameters, including the nature of the service (e.g. web service technologies, service registry,

web portal, and collaboration tools), automation, frequencies, access rights, security level.

- Reaching an agreement on a final list of purposes for information exchange.

The abovementioned tasks were expected to be accomplished with the following outputs:

Expected outputs	**Output reached: yes/no; reference chapter/annex for results discussion**
List and description of selected use cases	Yes, see Annex III
List and description of information services supporting the selected use cases	Yes, see Annex IV
List and definition of purposes related to the information services	Yes, see Annex V

2.2 Objectives

The Cooperation Project was expected to meet following objectives:

Objective 1: To define and agree on a selection of use cases with related information services and attached access rights (WP 2 and WP 4)

Objective 2: To define common data formats and semantics (WP 5)

Objective 3: To contribute to the cost-benefit analysis of Integrated Maritime Surveillance (WP 3)

Of these objectives, Objective 1, with the exception of access rights, falls under the responsibility of WP 2. A table of predefined Output and Result Indicators is presented in Annex II with a summary of delivered outputs and results.

3 Description of Use Cases

The use cases provide scenarios demonstrating how the information sharing environment is used and how to meet the user's requirements. The use cases cover all seven user communities and are relevant to all sea areas. WP 2 found that there was no requirement to differentiate between sea areas, so the use cases are generic in this respect.

One finding was that it is important to connect information sharing with the operational aspect and make the use cases narrative in order to understand why the use case/scenario is relevant, and that information sharing is done for a reason.

It became apparent very early on that there were many stakeholders in the use cases and that the cases therefore needed to be tailored for multiple uses. The obvious customers were the other WPs, but for partly different reasons. This meant that coordination with others was crucial when developing the use cases.

3.1 High-Level Use Cases

The chosen method was to describe a "High-Level Use Case" containing three processes describing the overall performance of how the information sharing system works. The three process levels are:

- **Baseline Operations**

This level describes "Everyday monitoring of events in the maritime domain", or "Behaviour monitoring". The purpose of this process is to ensure the lawful, safe and secure performance of maritime activities. Furthermore, to detect anomalies (detection of possible non-compliance) and other triggers/intelligence to improve decision making for the use of response capabilities (e.g. targeting of inspections). This level also contains "simple" response to single incidents or actions within the maritime domain – everyday operations.

- **Targeted Operations**

The "Targeted operations" level describes operations planned in advance towards a specific activity. The purpose of this process is to react to or to confront specific threats to sectorial responsibilities as discovered in risk analysis/intelligence gathering processes. Will give support to operational decision-making when employing operational assets.

- Response Operations

Response to major incidents, events or accidents. The purpose would be to respond to events affecting many actors across sectors and borders and with a potentially major impact on, e.g., the environment and economy.

Within these three levels of operations, it would be possible to find and describe sectorial needs for information and sharing, what kind of overall services are needed and also identify potential improvements of the information sharing environment on a high level. The High-Level Use Cases would also help to put the sectorial or detailed use cases into perspective and provide a firm basis for services identification.

3.2 High-Level Services

WP 2 also introduced the term High-Level Services (HLS). HLSs are services that trigger or support the High-Level Use Cases. They describe what overarching services may be used for each event. The events are the link between high-level use cases and the more detailed use cases. Five High-Level Services are described in Annex III.

3.3 Use Cases (detailed – sectorial)

WP 2 selected the nine use cases developed by the TAG as a starting point for further work. After comparing these against the use case "master list" (93-list), the decision was taken that the use cases selected that were representative of all user communities should be kept to be further developed and that these could effectively serve their purpose of driving the WP2 work forward. The original numbers were kept for future reference.

The template that was used to further develop the use cases indicates (among other things): what triggers the use case; who are the actors; what can go wrong and why, and finally, if there is a potential for CISE improvement.

The nine use cases are described in Annex III.

4 Description of Information Services

In order to simplify and understand the connection between Use Cases and Services a generic operational model was created. The model is the same regardless of the use case applied or which sector you belong to. Basically, the roles and products are the same, and the process of getting there is the same regardless of borders or sectors. This finding may simplify CISE development in the long run, and identification of where and how existing platforms/systems such as SSN, EUROSUR, SW and MARSUR fit into the CISE is easier to understand.

4.1 The process

1. For each use case:

a) *Develop a generic operational process model (roles, activities, input data, output data, description);*

b) *Define the services necessary to support it* (purpose, description, input data, output data, pattern);

i) *Define a task service for each activity* (more if necessary to support the main activity);

ii) *Define the necessary entity services* (considering the information needed as input for the activity), and;

iii) *Define the necessary support services* (if additional processing of the input data is needed).

2. Refine and complete each service definition.

4.2 Roles and Services

The three generic service types are:

- *Task Services* (services that define a specific Function – "What do you want to do?")

- *Entity Services* (manage access to operational entities; provide the information needed to implement the tasks)

- *Support Services* (execute operational rules to support operational decisions)

The different Roles are:

- Intel Provider

- Analyst

- Decision Maker

- Executor

Only eight use cases were used in this process. UC 37 was considered to be a service in itself and was therefore not used. UC 37 is however not deleted – it is needed for other purposes.

5 Purposes Related to the Information Services

The list of purposes is meant to define the objectives that different user communities have for information exchange through the services. Based on the list, it is possible to elaborate an access rights matrix and to design services with appropriate access right models.

The data sets are defined in relation to the TAG data matrix.

The list of purposes is presented in Annex V.

6 Conclusions

- The CISE is not only a technical issue – the Use Case development and Services work clearly revealed that the improvement of information sharing is very much tied to operational procedures and cultural developments. CISE development should therefore have integrated operational user demand and operational user requirement support when developing technical solutions.

- The generic operational macro-model used in the service identification work may be used for further technical development work. This will simplify routines, procedures and data formats as well as technical solutions. Ultimately, it will also simplify the work to achieve common standard operational procedures.

- Entity services should be common to all sectors. AIS information as an entity service, for example, is used by many users for different purposes – often as an important part of a support service. This will simplify standardization work, access right work and correlation work.

- The introduction of common, often-used Task Services should be considered. This may reduce the number of misdirected queries, improve the quality of response, and improve the speed of obtaining information.

- The establishment of an interaction network with common standards across sectors, borders and regions would facilitate the planning execution and evaluation of everyday work, use of operational assets, and support decision making. The common standards and interaction tools would be nationally implemented in NCCs, operation centres or wherever suitable. They would include HQ video and audio, map-sharing and other interaction tools.

- Development of common risk analysis and anomaly detection tools and sharing of best practices would facilitate early warning in all sectors and reduce the amount of unknown information. Sharing should be across sectors and borders.

7 Recommendations

- The WP2 work should be considered in the future work of other WPs. There may, however, be situations where the continued CoopP work may require further information on the WP 2 deliverables. The results may then be amended or complemented in line with new findings and requirements. Amendments must be approved and coordinated.

- As stated above, the development of the CISE should be user-driven and supported by relevant technology. Therefore, it is essential to maintain the operational–technical link in further development work.

- If only implementing parts of the CISE is a viable option, the WP 2 work indicates that operational developments (including access rights work) together with common data formats and semantics would give better results initially than common technical solutions. The best results, however, would be achieved if the procedural, technical and operational aspects were developed in parallel.

- In order to reduce possible rivalry between CISE development and existing systems for information exchange, CoopP may consider adopting the view that existing systems such as SSN, MARSUR, EUROSUR are, from the CISE viewpoint, “support services” using “entity services” also used by other actors to provide a better perception of what is going on in the maritime domain.

Annexes

Annex I List of Acronyms and Abbreviations

Annex II Meetings Summary

Annex III List of Use Cases

Annex IV List of Services

Annex V List of Purposes

Annex I – List of Acronyms and Abbreviations

AIS	Automatic Identification System
BLUEMASSMED	Pilot Project for the Integration of Maritime Surveillance on the Mediterranean Area and its Atlantic Approaches
BMM	See BLUEMASSMED
BSMF	Baltic Sea Maritime Functionalities
CISE	Common Information Sharing Environment
CleanSeaNet	Near-real-time satellite-based oil spill and vessel monitoring service
COI	Contact of Interest
CoopP	Cooperation Project Maritime Surveillance
CSDP	Common Security and Defence Policy
DG MARE	Directorate-General for Maritime Affairs and Fisheries
EEA	European Economic Area
EMODnet	European Marine Observation and Data Network
EMSA	European Maritime Safety Agency
ESA	European Space Agency
EU	European Union
EUROPOL	European Police Office
EUROSUR	European Border Surveillance System
FP7	EU Seventh Framework Programme for research and technological development
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GMES	Global Monitoring for Environment and Security
IA	Impact Assessment
IMDatE	Integrated Maritime Data Environment
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations
JRC	Joint Research Centre
LRIT	Long-Range Identification and Tracking of ships system
MARSUNO	Pilot Project: Maritime Surveillance North
MSEsG	Member States Expert sub-Group
POV	Pre-Operational Validations
SafeSeaNet	Vessel traffic monitoring and information system
SAR	Search and Rescue
SEIS	Shared Environmental Information System
TAG	Technical Advisory Group
THETIS	Information system for the Port State Control inspection regime of ships

User Communities	Border control, maritime safety and security, fisheries control, customs, marine environment, general law enforcement and defence
VMS	Vessel Monitoring System
WP	Work Package

Annex II – Meetings Summary

The attainment of project objectives under the responsibility of WP 2 was measured using the following output and result indicators. The following table gives a summary of the delivered outputs and results.

Output Indicators:	**Delivered Outputs**
Number and reports of meetings organized (working groups/sub-groups meetings, meetings between maritime authorities executing different maritime functions) and number of participants.	- Four WG meetings (27-42 participants) - One coordination meeting (6 participants)
Results Indicators:	**Delivered Results:**
All use cases together cover all participating sea basins and user communities. Use cases are representative of the main functionalities that the CISE is expected to perform in the future. The indicator is considered reached when these conditions are met.	Objective achieved
Number and nature of use cases. Target value to be defined in a Steering Committee after maximum 2 months following the start of the project.	3 high-level use cases 5 high-level services 9 use cases
Number of related information services. Target value to be defined in a Steering Committee after maximum 2 months following the start of the project.	Not relevant
List of purposes. The indicator is considered reached when a finalized list has been submitted to the TAG.	Objective achieved

Annex III – List of Use Cases

A. High-Level Use Cases, v 3.1

"Baseline operations"

Details	Process Description
"Baseline" Everyday surveillance and information sharing	Everyday monitoring of events in the maritime domain or "Behaviour monitoring".
Purpose	To ensure the lawful, safe and secure performance of maritime activities. Furthermore, to detect anomalies (detection of possible non-compliance) and other triggers/intelligence to improve decision making for the use of response capabilities (e.g. targeting of inspections).
Description	Each user community or actor monitors its own responsibilities. Basic data and sharing of information in accordance with agreements; cross-sector and/or cross-border sharing are typical requirements. Use of national and cross-sector information tools and sensors. The process also includes sector-specific data exchange requirements, procedures and systems defined in specific EU or international regulatory frameworks. Maximize information sharing to increase awareness and to promote decision making. Use of pre-emptive actions and decision making to minimize the need for "response operations". Baseline operations may include action against single events or minor actions, such as response to SAR situations, action against a detected oil spill from a single ship, detection and seizure of non-declared cargo, routine fishery inspection work with detection of infringement en seizure, boarding and inspections for different reasons, and so on. - Use of national surveillance sensors shared with others as required - Use of common available data sets/services region-, EU- or worldwide such as e.g. AIS information - Use of agreed incident reporting systems - Use of sector-specific communication procedures and networks.

	- Use of sector-specific data exchange systems and services.
Priority	*(High/Medium/Low)*
Frequency	Ongoing (always).
Potential for CISE improvement	This is a high-level use case that basically describes "Everyday Operations". Improvements in this area will affect all other activities. It will enable better indication of unlawful, unsafe and unsecure activities, better planning, better use of operational assets and quicker response times. This is clearly indicated in all other use cases. Examples: - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common format for information and/or data from sensors - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies across sectors and borders. - Common rules for history input to, e.g., databases

"Targeted Operations"

Details	Process Description
"Targeted" surveillance and information sharing for targeted operations	Targeted operations towards a specific activity.
Purpose	To react to or confront specific threats to sectorial responsibilities as discovered in risk analysis/intelligence gathering processes. Will give support to operational decision-making when employing operational assets.
Description	Typically sector-driven operational activity *planned in advance*, often with operational assets deployed with the aim of detecting and preventing violations of the safe, secure and lawful performance of maritime activities within own sector. May be limited in time, space and geography. Sector cooperation, cross-border, regional or EU wide, may occur. *Operations triggered by sector risk- or threat analysis or as a "deterrence"*. Even though operations are sector driven, information sharing across sectors occurs. Examples may include and be exemplified by: - JDPs (NAFO, NEAFC, ICCAT…) in international and EU waters. - Operation ATALANTA - Operation MINERVA, INDALO
Priority	*(High/Medium/Low).*
Frequency	As required - intelligence and/or risk analysis driven.
Potential for CISE improvement	The key issues for success in this high-level use case are cross-border cooperation and interaction within sectors as well as all sector-/border information sharing. Common interactive communication and collaboration tools are of great value in planning operations and making best use of operational assets. Examples: - Common collaborative tools (voice, HQ video) - Improvement of availability of information.

	- Clearer rules for inter- and intra-sector sharing mechanisms (access rights and security levels) - Common standard operating procedures across sectors and borders - Common format for information and/or data from sensors - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

"Response Operations"

Details	Process Description
"Response" Operations	Response to major incidents, events or accidents.
Purpose	To respond to events affecting many actors and with a potentially major impact on, e.g., the environment and economy.
Description	Typically a response to complex events involving several actors from different sectors and across borders. Events occur suddenly, without warning. Decision making under time pressure. Complicated cross-border and/or cross-sector decisions. Potentially huge values at stake – environmental, financial and human lives. Huge need for operational coordination across sectors and borders. Often large amounts of operational assets involved. Examples of this process may include: - "Estonia" or "Costa Concordia" -type ferry disaster - Tanker collision with large passenger carrier - Sudden massive migration flow due to specific events, e.g. natural disaster or war - Terrorist attack or threat of attack with weapons of mass destruction - Cross-border efforts to stop large amounts of drugs with unclear destination from reaching the EU - Fishing gear conflicts and conflicts between groups of fishing vessels (which could lead to the need for immediate intervention (possibility of vessels attacking each other) ….. Note: "Normal" incidents, such as a single SAR case, a single fishing violation or a case of smuggling may also be included under "Baseline Operations" above.
Priority	*(High/Medium/Low).*
Frequency	Irregular. Frequency based on a "case-by-case" basis. Predictions not possible or event may be totally unforeseen. Operations may be needed over long or short periods of time.
Potential for CISE	- Establishment of common collaboration tools

improvement	- Knowledge of availability of operational assets across sectors and borders - Established, frequently trained routines across sectors and borders for all sorts of intervention - Common Standard Operating Procedures (SOPs) - Common or shared support services to detect anomalies and risks - Immediate access to an extended array of data that is normally not included in the maritime field. - Cross-border or cross-sector agreements covering extensions of “normal” latitude.

B. Events describing "High-Level Services"

Events are developments of the above high-level use cases. They describe what overarching services may be used for each event. The events are the link between high-level use cases and the more detailed use cases.

1. Situational awareness

Details	Event Description
Process Name	Collecting, processing and sharing basic maritime data
Event Name	Sector Recognized Maritime Picture or situation (RMP)
Description	Sector, national, regional and/or EU-wide services used to provide a recognized maritime picture for a sector. National or regional maritime situational awareness may be tailored for sector or cross-sector purposes depending on national legislation and bi- or multilateral agreements. Information exchange and sharing are in line with this principle. Basic data sources or services contain open information. It is important that the amount of services used provides as much open information as possible. Map services, weather services, tools for visualization and compilation are examples of means to improve quality of information. Typically, basic and additional information is shared on a regular basis. This event may be divided into two levels: 1. Acquisition of Common Basic Maritime Situation (level 1) 2. Elaboration of a Consolidated Common Maritime Situation (level 2) In the 1st level, actors are existing institutional communities acting in the acquisition domain (e.g. EMSA and Members States' communities). At this level, there is no sensitive information and there is no limitation on sharing information within the CISE environment. The 2nd level requires additional information, such as: • Information on the travel, cargo… • Worldwide information history (ships, routes , …) • Additional data from non-permanent data sensors (naval, aerial, space sensors)

	• Information from maritime databases (ship characteristics for classification/recognition/identification…) This additional information is collected in order to complete the picture, to avoid duplication of ships and routes, to detect falsification of ship's identity, and to perform the other necessary correlations for integrity control and for the validation of all information of the CCMS. This function cannot be merged with the acquisition function since it needs to correlate basic data with additional data (for example fishing vessel location). The function is activated in routine mode and represents Level 2 of the operations flow. It can be activated in prevention mode; in this case, the procedure applied for the surveillance of the zone can be classified as sensitive information by the Member States.
Frequency	Everyday activity (H24).
Potential for CISE improvement	See high-level use case "Baseline" above, and detailed use cases, especially No. 37.

2. Anomalies

Details	Event Description
Process Name	Detect anomalies, incidents and conduct risk assessment and analysis in the maritime domain
Event Name	Triggers for operational action
Description	Manual and/or automated detection of an incident that falls outside the frame of "normal operations". Typically detected within own sector work. May require action from other sectors. Services used may include sector- or domain-wide anomaly detection tools, risk analysis and planning tools. Typically, basic and additional information is shared on a regular basis.
Frequency	Everyday activity (H24).

Potential for CISE improvement	- Sharing of anomalies and detected risks throughout sectors and borders. - Common or “best practices tools” would be of great importance for discovering threats to the lawful, secure and safe conduct of maritime and marine activities. This would improve the performance of authorities in different sectors. - Proper sharing mechanisms are essential (tech, SOPs and legal conditions)

3. Operational availability

Details	Event Description
Process Name	Availability of assets
Event Name	Knowledge of availability of operational assets
Description	Cross-border and cross-sector knowledge of availability of assets available for operations. Knowledge of planned operations in the maritime domain. Common standards (SOPs) and communication tools needed. A service for sharing this information (including contact information) is essential. Typically, basic and additional information is shared on a regular basis.
Frequency	As required
Potential for CISE improvement	- Will improve the knowledge availability of assets which, in turn, will reduce patrol cost, overlapping surveillance costs and readiness cost - Great potential for savings in terms of lives, environmental and marine values, etc.

4. Extra ordinary

Details	Event Description
Process Name	Extended information sharing
Event Name	Increased information availability

Description	When major incidents or accidents occur there is a need to coordinate assets from several sectors and nations. Decision making across sectors and borders is required. Information sharing outside normal patterns is required. Services should be designed to share information accordingly. Basic and additional information is to be shared as well as restricted as required.
Frequency	As required
Potential for CISE improvement	- Will enable quicker and more accurate decision making under time constraints, which will save time and costs during operations. - More accurate perception (several aspects) of the situation before decision making.

5. Virtual interaction

Details	Event Description
Process Name	Virtual Interaction
Event Name	Virtual User Groups
Description	There is a need for virtual (online voice and video) interaction between decision makers, operators and on-scene commanders/coordinators when responding to events, coordinating resources and planning activities, both cross-border and cross-sector. The aim is to share information from person to person or between groups in order to attain a real-time recognizable picture of the event, whether for planning purposes, or during execution of a response operation. Services to facilitate this would include high quality video and audio streaming, video sensor information and document presentation. Services would enable pre-defined tailored user groups for specific purposes.
Frequency	As required. The more frequent the use, the better the environment for information sharing, planning and decision making.

Potential for CISE improvement	- Better trust and confidence between authorities - Easier to connect operational networks in case of accidents - Better operational planning, saving time and money - Potentially less risk of error when interacting person to person - More robust decision-making

C. List of Use Cases for baseline maritime environment

Use Case ID 13b	Description		
Goal	Inquiry on a specific suspicious vessel (cargo related)		
Operational situation / Trigger	Intelligence driven information reveal that a ship´s cargo is illegal, dangerous or in other ways in breach of rules and regulations.		
Lead Actor	Border Control, Customs, General Law Enforcement, Defence		
Additional Actor(s)	Defence, General Law Enforcement, Marine Pollution Preparedness and Response/Marine Environment		
Pre-conditions	Baseline, Targeted, Response.		
Post-conditions	Sector decision makers made decision to act or not (and with what resources)		
Failure/Outcome	Failure	Outcome	Condition leading to outcome
	1/ Failure to receive the requested information, information not precise, not relevant or not provided in a timely manner	Uncertainty if cargo is illegal or not 1/ Illegal cargo will reach its destination 2/ OP resources not deployed to	1/ Poor information sharing 2/ Request not directed to the correct Authority 3/ Request not clear 4/ Restricted information

		verify cargo 3/ Lack of decision support leads non-optimal management of resources	
	2/ Failure to respond to suspicious cargo shipments	1/ Cargo reaches destination 2/Excise duties not paid	1/ Lack of decision support leads to non-optimal management of resources. 2/ OP resources not deployed effectively to verify cargo.
	3/ Failure to adequately address security levels	1/Poor information security procedures	1/ Inadequate or faulty security information guidelines /rules
Flow of Events	The actor responsible for detecting illegal cargo gets an information alert signal from one or more systems. The information alert may come from e.g. anomaly detection services, other actors systems or other intelligence sources. The actor queries the system to get replies from other sources of information in order to confirm own sources. The outcome of this process will be a decision on intervention or not. It will also initiate sharing of additional information.		
Alternative Scenarios	1) Uncertainty if cargo is illegal: the decision to control is based on targeting cargo (Pre-arrival data) with a view to enrich intelligence and justify intervention as described in “flow of events”. 2) Unwanted effects on society: solving the unwanted effects on community could be achieved by improving tools, enhancing the organisation of customs services and multiagency cooperation (medium term process).		
Procedures	SCOPE: ANTI SMUGGLING and commercial fraud (misdeclarations of goods), and any other cargo related illegal activity. **CASE: CREW FRAUD / VESSELS SEARCH** Type of intervention: search of vessels at sea/port (once ship docked) -- RISK		

	ANALYSIS EXCLUSIVELY: • Risk indicators: composition of crew, type of vessel, routine checks (Are crewmembers known to the Authorities? What is the ship history...) • As far as possible (framework NAPLES II): coordination with other Member States Customs services to prevent search the same parts of the vessel in case of calls in two European seaports successively -- commodities targeted: cigarettes, narcotics, fake white goods, fake clothing etc..
Traceability	A database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities.
Inputs Summary	«Flagged» by anomaly detection, risk analysis from own or other authority, Shared pre-arrival data, Knowledge of resources for intervention - Basic Ship Data (position, voyage and permanent data) - Additional data (cargo and crew/passenger)
Output Summary	Database feed: - Inspection report including follow up activities - Detailed report regarding cargo, persons on board - Lessons learned
Potential for CISE improvement	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intrasector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders.

Use Case ID 13c	Description		
Goal	Inquiry on a specific suspicious vessel (crew and ownership related)		
Operational situation / Trigger	Intelligence sources alert that persons on board a vessel could be illegal or have criminal background. Uncertainty over the ownership of the vessel.		
Lead Actor(s)	Defence, Border control, General Law Enforcement		
Additional Actor(s)	Defence, Border control, General Law Enforcement		
Pre-conditions	Baseline, Targeted, Response operations		
Post-conditions	In case of positive response, relevant authorities alerted. Make an inspection as soon as possible. Seek additional support from other Agencies/countries as necessary		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	Failure to receive the requested information, not relevant or not provided in a timely manner	The inspection of the crew is not done, the ship continues its voyage. 1-Criminals achieve their objective 2-Law is not upheld	1/ Restricted information2/ Request not directed to the Lead organisation /Agency 3/ Request not clear
	Information is not precise	1/ Poor decision making process 2/ Intelligence is compromised. Information on crew and/or	1/ Request not clear 2/ Information received not relevant

		ownership suspect	
Flow of Events	The actor responsible of detecting illegal crew activities gets an alert triggering a response. This alert may come from different sources e.g. from an intelligence source or from an information or alarm from any Community Authorities or from another Member State. The outcome of this process will be a decision on intervention or not. It will also initiate sharing of additional information.		
Alternative Scenarios	1) Uncertainty if crew is illegal: the decision to control is based on targeting vessel (Pre-arrival data) with a view to enrich intelligence and justify intervention as described in “flow of events”. 2) Unwanted effects on society: solving the unwanted effects on community could be achieved by improving tools, enhancing the organisation of customs services and multiagency cooperation (medium term process).		
Procedures	Identify the origin of the ship and gather all relevant information about the ship, port of departure, cargo, and crew. Seek additional information about the ship from other Member States. (Personal data information sharing must be compliant with law.) State precisely what information is needed, and give a brief explanation about why the information is required. Be sure the information is encrypted or sent by a secure way. Information sharing between users must be by secure means. Confidence building is critical between users.		
Traceability	A database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the		

	relevant authorities
Inputs Summary	«Flagged» by anomaly detection, risk analysis from own or other authority, Shared pre-arrival data, Knowledge of resources for intervention. - Basic Ship Data (position, voyage and permanent data) - Additional data (cargo and crew/passenger)
Output Summary	Database feed: - Inspection report including follow up activities - Detailed report regarding cargo, persons on board - Lessons learned
Potential for CISE improvement	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders.

Use Case ID 25b	Description		
Goal	Investigation of antipollution situation (law enforcement)		
Operational situation / Trigger	A vessel is suspected of polluting. - Sighting by satellite - Sighting by aircraft - Sighting by surface vessel - Sighting from coast line - Reported by vessel polluting - Reported by other sources		
Lead Actor(s)	Marine pollution preparedness and response/Marine Environment		
Supporting Actor(s)	General law enforcement, Maritime Safety		
Pre-conditions	1/ Pollution sighting is verified 2/ Baseline, Targeted and Response operations (in case of environmental disaster such as The Prestige)		
Post-conditions	In case of positive response, relevant authorities alerted. Make an intervention as soon as possible. Seek additional support from other Agencies/countries as necessary 1/ Pollution contained and analysed to determine source for possible prosecution. 2/ Database feed for lessons learned, action taken reporting		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	1/ Pollution not contained	1/ Polluter not prosecuted	1/ Insufficient number of sensors or poor quality

	2/ Analyses not satisfactory	2/ Environmental damage to sea life and shoreline	2/ Insufficient anti-pollution resources 3/ Insufficient operational coordination 4/ Insufficient law enforcement procedures
	1/ Failure to receive the requested information	1/ Pollution not detected. 2/ Environmental damage to sea life and shoreline 3/ Environment affected, polluter not prosecuted	1/ Poor information sharing 2/ Request not directed to the correct Authority 3/ Request not clear 4/ Restricted information 5/ Poor sensor quality 6 / Inadequate Alert systems
Flow of Events	Responsible authorities alerted of a suspicious pollution event. (System alerts to each member state of the presence of a suspicious vessel in their territorial waters). The alert may come from a number of sources e.g. AIS system, intelligence source, from other member state or from a vessel that has observed some irregular activities. The own member state could ask to the system for any additional information about the vessel. If the system has any important information regarding the vessel, the complete information is reported: name, cargo, ownership, activity, position, previous pollution problems. - Containment plan initiated, - Response vessels mobilized - Response aircraft mobilized - C2 in place		

	- Interagency coordination group meet and decide on best course of action - Actions carried out - Event close
Alternative Scenarios	- Time lag in reporting - Response vessels and aircraft not available. - Poor C2 - No pollution response plan - Inter-Agency rivalry
Procedures	- System detects the presence of a vessel suspicious of polluting. - The actor introduce the identification number, or the name of the vessel in the system - The system looks for any relative information and asks for the other users about this issue. - The information is given to the Lead Actor
Traceability	A database of suspicious vessels suspected of polluting, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected of (or have caused) pollution should alert the operator to report presence of vessel to the relevant authorities
Inputs Summary	- Report or sensor input on pollution - Drift model usage - Pollutant data (type, substance, volume etc) - Ship data (basic and additional, cargo, ownership) - Response resources (national and cross border) - C2 structure cross border and cross sector
Output Summary	- Alert to shipping and shore authorities

	- Successful prosecution of polluter - Financial claims settled - Database input (lessons learned, Pollution reports)
Potential for CISE improvement	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders.

Use Case ID 37	Description		
Goal	Monitoring of all events at sea in order to create conditions for decision making on interventions		
Operational situation / Trigger	Sensor information e.g. coastal radars and cameras, aerial sensor information and AIS) relaying information in real time or delayed), and other information services (anomaly detection services, databases) and systems such as EUROSUR or MARSUR.		
Lead Actor(s)	All User Communities		
Supporting Actor(s)	All User Communities		
Pre-conditions	Baseline		
Post-conditions	Recognized maritime picture		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	1/ Technical failures	1/No data input 2/ Less than optimum response	1/ Low quality sensors/systems 2/ no redundancy in systems 3/ Lack of contingencies
	2/ Operators fail to detect threats	The threat is not identified	1/ Lack of training 2/ Lack of common SOPs
	3/ The event is not detected hence remains unknown	No intervention possible	1/ Training and/or op posture 2/ Technical faults
	4/ The event is detected but the information is not integrated into the system	No intervention possible	1/ System integration not adequate
	5/ The information is integrated but not	No intervention possible	1/ Operator fault

	sent to the relevant authority(-ies)		2/ System integration/ architecture inadequate
	6/ Failure to detect Contact of Interest (CoI).	CoI is not detected	1/ Incomplete RMP. Poor interagency cooperation. Inexperienced operators
Flow of Events	Monitoring systems are always sending information (tracks and pictures), that must be interpreted by a trained operator. In case of anomalies in vessel behaviour, the operator triggers a process for intervention. - Information Services to deliver information on basic, additional and restricted information with a high level of reliability. - Tools and functional services to process basic ship data in order to produce risk analyses and anomaly detection - Produce alerts to other cross sector and borders - Operators and decision making procedures to be able to act if necessary - Sharing of information in accordance with SOPs and agreements cross border- and sector - Produce history input to databases		
Alternative Scenarios			
Procedures	The reports are processed and related information is fused with other data / information in accordance with SOPs of authorities involved.		
Traceability	Data coming from all available sensors are displayed and fused together for operators or automatic evaluation.		
Inputs Summary	Sensor input (radar tracks, AIS, Cameras, satellites, UAVs etc.)		
Output Summary	Anomalies in vessel movements detected and operational intervention considered.		
Potential for CISE improvement	This is the use case which basically describes “Everyday Operations”. Improvements in this area will affect all other activities. It will allow for better indications of unlawful, unsafe and unsecure activities, better planning, better use of operational assets and quicker response times. It is closely related to the High-Level Use Case “Baseline Operations”.		

	Examples: - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common format for information and/or data from sensors - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

Use Case ID 44	Description		
Goal	Request for any information confirming the identification, position and activity of a vessel of interest		
Operational situation / Trigger	Member state authorities have an interest in knowing the current position of a vessel, its activity, identification etc. The information could be requested because: - The vessel is subject to police investigation - The vessel is suspected of involvement of irregular migration, drug smuggling or other cross border crime - There are evidences of pollution from the vessel - The vessel owner is subject to an adverse legal judgement - The vessel is subject to an investigation from an intelligence agency		
Lead Actor(s)	All user communities		
Supporting Actor(s)	All user communities		
Pre-conditions	Baseline, Targeted and Response operations		
Post-conditions	The information can support an intelligence process, a police investigation or even confirm (in a positive or negative way) a suspicious track. Supports decision on intervention or not.		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	1/ The information is not provided in a timely manner	1/ The investigation is compromised. 2/Relevant Authorities not notified in a timely manner leading to non-intervention 3/ An	1/ Request not directed to correct authority 2/ Classification mismatch 3/ Incomplete RMP 4/ Poor SOP's

		environmental disaster occurs.	5/ Inexperienced operators
	2/ Information not provided	1/ The investigation does not take place . 2/ Relevant Authorities not notified in a timely manner leading to non-intervention 4/ An environmental disaster occur.	1/ Failure to communicate through agreed lines of communications 2/ Classification mismatch 3/ Incomplete RMP 4/ Poor SOP's 5/ Inexperienced operators
	3/ Incorrect and not complete response	1/Time delay verifying request 2/ The investigation cannot continue 3/Relevant Authorities not notified in a timely manner leading to non-intervention 4/ CoI lost	1 / Failure to communicate coherently 2 / Lack of sensor- or database information 3/ Lack of proper information sharing functions 4/ Lack of SOPs 5/ Incomplete RMP

			6/ Inexperienced operators
	4/ The information is not updated	1/ decision making process compromised 2/ Poor utilisation of resources	1/ Communication failure 2/ Lack of proper information sharing functions 3/ Lack of SOPs
Flow of Events	User needs to know position of the vessel. The system checks the AIS signals and other resources and the vessels position is verified Additional information is provided by other sensors or Regulatory authorities		
Alternative Scenarios	-		
Procedures	User seeks information for the position, activities or the identification of a suspicious vessel The system checks and provides the position (and other related basic maritime data – e.g. from AIS). Additional available information (additional and restricted data) is provided by functional services, e.g. current identification, former names (in case), current activity, historical activities.		
Traceability	- A database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities		
Inputs Summary	System input - All available information services - All available functional services		
Output Summary	- Decision support on intervention or not - Input to historic databases		
Potential for CISE	- Common correlation services		

improvement	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

Use Case ID 57	Description		
Goal	Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance (Baseline and Targeted operations)		
Operational situation / Trigger	- Need for enhancing or complement surveillance in areas where surveillance is poor or there is a specific surveillance need. - Support for decisions where to deploy additional surveillance assets		
Lead Actor(s)	All user communities		
Supporting Actor(s)	All user communities		
Pre-conditions	- Policy on info sharing between actors both Nationally and Internationally - Common data formats - Agreed MOU's leading to agreed SOP's - Secure lines of communication		
Post-conditions	- Sectors/ Nations share information on own surveillance capacities and capabilities		
Failure Outcomes	Failure	Outcome	Condition leading to outcome
	1/ Info not shared	1/ Decision making process compromised 2/ Poor RMP 3/Uncertainty about surveillance capacities of partner authorities in a given sea area to plan basic tactical	1/ Lack of inadequate procedures for sharing information 2/ Classification levels 3 / Request not directed to the correct Authority 4/ Request not clear 5/ Restricted information

		surveillance 4/ Lack of decision support leads non-optimal management of resources 5/ Operational potential not achieved 6/ Less effective planning of operations	
	2/ Incomplete RMP	1/ Higher risks for illegal maritime events and accidents	1/ Inadequate information transferred
Flow of Events	- Request for information received through agreed lines of communication - Request is comprehensive in nature - Information transferred through agreed lines of communication in a timely manner - Information transferred is comprehensive in nature Information transferred is pertinent to the request		
Alternative Scenarios			
Procedures	- Each sector / Actor monitors own surveillance needs for baseline operations. When surveillance situation needs enhancement, operators send request to others (cross sector and/or border) for sharing and coordination of surveillance results/ assets.		

	- When a planned operation is to occur (targeted operations), the lead organisation/agency liaise with other actors in the operation to ensure conformity to agreed actions/timelines Information exchange only made through secure channels.
Traceability	-
Inputs Summary	- Request from actor in need of enhancement of surveillance - Surveillance needs for a planned operation
Output Summary	- Answer to request of surveillance enhancement - Surveillance plan for planned operations - Deployment plan for surveillance assets - Coordination of surveillance assets
Potential for CISE improvement	- Common correlation services - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

Use Case ID 70	Description		
Goal	Suspect Fishing vessel/ small boat is cooperating with other type of vessels (m/v, Container vessel etc.)		
Operational situation / Trigger	A fishing vessel / small boat is suspected to have suspected activity with another vessel.		
Lead Actor(s)	General Law enforcement, Customs, Fisheries control, Defence, Maritime Safety		
Supporting Actor(s)	General Law enforcement, Customs, Fisheries control, Defence, Maritime Safety		
Pre-conditions	Baseline, Targeted, Response operations.		
Post-conditions	- All available information collected - Support for intervention decision provided - Operational assets alerted - Event recorded - Lessons learned and other information provided to databases		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	1/ The information is not provided in a timely manner	1/ The investigation is compromised. 2/ Relevant Authorities not notified in a timely manner leading to non-intervention	1/ Request not directed to correct authority 2/ Classification mismatch 3/ Incomplete RMP 4/ Poor SOP's 5/ Inexperienced operators
	2/ Information not provided	1/ No Investigation takes place.	1/ Failure to communicate through agreed lines of

		2/ Relevant Authorities not notified	communications 2/ Classification mismatch 3/ Incomplete RMP 4/ Poor SOP's 5/ Inexperienced operators
	3/ Incorrect and/or not complete response	1/ Time delay verifying requests 2/ Relevant Authorities actions compromised 3/ CoI lost	1 / Failure to communicate coherently 2 / Lack of sensor- or database information 3/ Lack of proper information sharing functions 4/ Lack of SOPs 5/ Incomplete RMP 6/ Inexperienced operators 7/ Availability of

			operational assets
Flow of Events	Intelligence alert to the presence of a fishing vessel/small boat suspected of collaborating with other suspected vessels. The track of the fishing vessel is monitoring and if it is possible, an inspection should be carried out.		
Alternative Scenarios			
Procedures	- Identify the origin of the fishing vessel and gather as much information as possible about the vessel, port of departure, catch, and crew details. - Same procedure with the other collaborative vessel if the identification is known. - Draw historical and current information on the vessel for input to the decision making process. - Specify the type of information required and the reasons why it is required - Information exchange by secure means... - Alert the relevant authorities.		
Traceability	- A database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities		
Inputs Summary	Basic, additional and restricted maritime traffic and additional information such as : - identification number of the fishing vessel - identification number of the collaborative vessel if possible - Catch - flags - crew if possible - suspect - last AIS signal		

	- last known verified position - History of both vessels
Output Summary	- All the identification data required - Tracks and other data over the event to feed databases
Potential for CISE improvement	- Common correlation services - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

Use Case ID 85	Description		
Goal	Anti-Piracy Maritime Surveillance and free navigation control: Merchant vessels at sea (outside Territorial waters) sends an alert that it is under Piracy attack		
Operational situation / Trigger	An alert is received by MS designated authority regarding a piracy attack of a ship entitled to fly its flag outside territorial waters		
Lead Actor(s)	Defence/Maritime Safety/ General law enforcement		
Supporting Actor(s)	Defence/Maritime Safety/ General law enforcement		
Pre-conditions	Response		
Post-conditions	Pirates fail to hijack ship. Pirates seized and brought to justice. All available information collected - Support for intervention decision provided - Operational assets alerted - Event recorded - Lessons learned and other information provided to databases		
Failure/Outcomes	Failure	Outcome	Condition leading to outcome
	1/ Insufficient amount of correct information available	1/ Slow decision-making and reaction time 2/ Pirates board vessel 3/ Human lives at risk	1/ Information sharing in real time insufficient 2/ Poor sensor- /data availability 3/ Improper SOPs 4/ Security levels- / agreements

			5/ Poor interagency cooperation
	2/ Difficulties to exchange restricted information in time	- See above	1/ Improper sharing mechanisms for restricted information 2/ Improper SOPs
	3/ Slow decision-making	See above	1/ Poor interagency cooperation 2/ Poor SOPs for interagency decision making under time pressure 3/ Inadequate means of communication and interaction between authorities
Flow of Events	- The Alert is received and immediately an operational emergency order is activated - Interagency cooperation is an immediate need - cross border and sector - Information flow to be very near real time with operations. Two way information flow		
Alternative Scenarios	-		
Procedures	- When a competent Administration receives notification of a ship security alert, that Administration shall immediately notify the State(s) in the vicinity of which the ship is presently operating. When a MS (Contracting Government) receives notification of a ship security alert from a ship which is not entitled to fly its flag, that MS shall immediately notify the relevant Administration and, if appropriate, the Member State(s) in the vicinity of which the ship is presently operating. - When the vessel that sends the security alert is located, the rest of the users of the system should activate an agreed common operational rescue		

	plan. - This operational plan should be similar for all members, over all in the case that the vessel is out of the territorial water. The responsibility for rescuing the vessel depends on the SAR (search and rescue) area in which the vessel is located. This country should provide an immediate response and seek additional assistance if required - If the vessel is in the SAR area of a third country. Several actions can be contemplated. The first action is to communicate the situation to that third state to ensure that it is alerted to the situation and has control of the situation. - Alert other actors to the possibility of supporting the third country in the operation.
Traceability	The Ship Alert Security System when activated, transmit a ship-to-shore security alert to a MS competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised.
Inputs Summary	- Security alert - Plans and SOPs
Output Summary	- Support to decision making - Communications - Record events - Database feed for history log and lessons learned
Potential for CISE improvement	- A common system for rapid operational/ tactical planning and co-ordination of assets reaching across sectors and borders. - Common correlation services - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders

	- Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases

Use Case ID 93	Description		
Goal	Detection and behaviour monitoring of IUU listed vessels		
Operational situation / Trigger	Surveillance of EU waters and ports, increased behaviour monitoring when target is found to be listed as IUU vessel.		
Lead Actor(s)	Fisheries Control		
Supporting Actor(s)	Defence, General Law Enforcement, Border Control, Customs.		
Pre-conditions	Baseline, Targeted, Response: Decision on action (sea inspection) or not. Action when detection in port..		
Post-conditions	Vessel refused port services, landing of fish, blockage of landed cargo.		
Failure Outcomes	Failure	Outcome	Condition leading to outcome
	Failure to detect presence of IUU listed vessel.	- Illegal fishing activity performed - Weakened deterrent effect for IUU activities	1/ Poor RMP 2/ Poor sharing/ knowledge of IUU list
	Failure to detect IUU vessel landing in EU port.	- Depletion of stock Negative Economic effects Negative effect on consumer rights - Illegally caught fish will be commercialized. Multiplication of resources needed to trace illegal	1/ Poor information exchange between actors (e.g. fisheries control and general law enforcement) 2/ Poor levels of information security 3/ Poor interagency cooperation

		commercialization following landing.	
Flow of Events	Actors should be aware of the existence of IUU list and have list of IUU vessels that is current... Upon detection of vessel, the vessel is cross checked with the IUU list. Action will be triggered when there is a positive cross check. Action can consist of : -intensified monitoring for decision making -sea inspection to check cargo and activity -when in port, prevention of services and landing of cargo		
Alternative Scenarios	-Intelligence gathering and mapping of organised illegal import chains -Enhanced monitoring of target vessel activities		
Traceability	Identify work products, models or documents that this use case is traceable to, for example, business rules, functional requirements, prototypes etc.		
Inputs Summary	Details on detection (identification) and activity of target Proposed actions and results of actions		
Potential for CISE improvement	- Common correlation services - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels) - Common standard operating procedures across sectors and borders - Common entity services (as many as possible) across sectors and borders - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history input to e.g. databases		

Annex IV – List of Services

SECTION A: Describing the process.

1 Explanation of the template

Each use case is described by a set of activities in the corresponding operational process model; each of these activities is then realized by a set of services. Both, the activities and the services, have to be defined, providing examples whenever necessary.

1.1 List of activities

For each activity in the operational process model encompassed by the use case under analysis, fill in the table below.

Activity	Role	Input	Output	Description/example	New entities
Short name for the activity (should be related to an activity chart)	to choose between: - Intelligence provider - Analyst - Operations decision maker - Operations executor	Main entities necessary for the activity	Main entities resulting from the activity	Textual description or example if necessary	

Note: The data entities used as input/output should come from the Information Model (presently the Data Matrix). Please add to the column “New entities” those that are needed as input/output but are not present in the Data Matrix

1.2 List of services

Each activity listed above will be realized by a specific ”Task service” through the composition of “Entity Services” (exchange of information) , “Support Services” (adding value to data by implementing specific algorithms or business rules) or even other Task services, as required to fulfill the purpose of the activity.

Services encompass operations which are used to realize the specific steps of an activity. Please identify all the necessary services to fulfill the purpose of each of the activities above,

and further define them in terms of the necessary operations and inherent input and output data, by filling in the table below.

The table below should be repeated for each task service in each activity, new rows may be added as necessary.

Service type	Name	Input	Output	Pattern	description
Task service	Simple name	Main entities used as parameters for the operation	Main entities provided by the operation	Choice between: - Pull - Pull delayed - Broadcast pull - Broadcast push	Textual description or example if necessary
Support service					
Entity service					

Eight of the nine use cases have been mapped against the principles described above. This will give an indication of which input and output is expected in each case by which community. The input in each case will give good guidance to elaborate with access rights in a number of dimensions. All is pointing to the present data matrix.

The list of services together with the high-level use cases and the use cases will be the primary source for designing the “List of purposes for information sharing”, which in turn will give guidance for further work with access rights.

SECTION B: Services to Use Cases

Eight use cases described – use case 37 is in this respect considered as a “service”, but will be kept as a use case for other reasons.

Use Case 13b	Inquiry on a specific suspicious vessel (cargo related)

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	ship (name, flag+history), passenger, crew list (+history), ownership (+history), voyage/routes (+history), suspected person, position, cargo, known criminal background on person on board	Intelligence report: anomaly, risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	collection of intelligence and field reports	will ask for other analysis from other intelligence provides	
analyse further info	Analyst	collection of intelligence and field reports	analysis report: consolidated intelligence report, recommendation		
provide further info	Intelligence provider	RFI: sighting, VHF contact, etc…	RFI reply	provide information from the field	
decide COA	Operations decision maker	analysis report	selected course of action		
update intelligence	Intelligence provider				
forward info	Operations	analysis report	action request or		

Activity	Role	Input	Output	Description/example	New entities
	decision maker	and selected course of action	notification (including the analysis report and selected course of action)		
issue operational instruction	Operations decision maker	analysis report, available assets, other operations in the area	set of operational instructions (how, who, when, why, where, what)		
Action	Operations decision maker	set of operational instructions	set of operational instructions (how, who, when, why, where, what)		
close operation	Operations decision maker	several situation reports	after action report		
update intelligence on closure	Intelligence provider				

List of services for the activity "analyse available information" + "collect and analyse further information"

Service type	Name	Operation	Input	Output	Pattern	description
Task service	Illegal cargo vessel automated targetting service		Any relevant information related with the ship, the transported goods or its crew.	-Intelligence report -Additional data for further risk analysis	Broadcast push	A list of suspected vessels making possible or easier an efficient control, at sea or at port, depending on the type and location of the vessel.

Service type	Name	Operation	Input	Output	Pattern	description
Support service	List of vessels suspected of transporting illegal goods		Any relevant data	A list of identified vessels	Broadcast push	An alert system resulting from matching/hitting functions, making possible a smart control in a context of important exchange of goods by maritime transport and of drastic budgetary cuts. Involves a data mining function.
Entity service	Vessels service		All informations related with the vessel itself (name, owner, flag, etc)	All informations related with the vessel itself (name, owner, flag, etc) with an historical overview	Broadcast push Or pull	Possibility to get all the informations enhancing the knowledge of suspected vessels on demand (research function)
Entity service	Voyage/route service		Port of departure, port of arrival, maritime roads, duration of each stop or trip, etc.	Geographical and chronological overview on the vessel trip and stops.	Broadcast push Or pull	Geographical and chronological overview on the vessel trip and stops. Possibility to visualise these information on a map.

Service type	Name	Operation	Input	Output	Pattern	description
Entity service	Events know by the port of control (break, etc.)		Events, facts	Particular events with consequences on the cargo.	Pull	Alert function on any particular events regading the vessel with consequences on the cargo.
Entity service	Logistics/supply chain details		All details related with the supply chain between the expeditor and the deliverer (actions operated by all stakeholders, controls).	Detailed information regarding the supply chain operations and actors (ex : nbr of cranes used to deal with the cargo)	Broadcast push Or pull	Historial list of all the stakeholders and what they did and how they operated it on the cargo and on the vessel.
Entity service	Location of the suspected vessel		AIS LRIT VMS Satellite images	Real time position of the vessel Historical of the position (voyage) Direction and speed of the vessel	Pull	Position of the vessel in the present , the past, and its anticipated road.
Entity service	Available partners, at sea or in port, for a potential control		-Patrol plans -Without notice operating services	Knowledge of available partners to operate a control.	Pull	Cross border coordinated operation between a provider of intelligence and an enforcement service.
Entity service	Dedicated means of communication		-Identification of partners (organisations, names, ranks,	CISE phone book, secured mail box, chat,	All	Communication tools making it possible or easier to contact and

Service type	Name	Operation	Input	Output	Pattern	description
			functions, phone numbers, e-mail address, fax) - Proper restricted level of protection	etc.		exchange with the right person in the right country in a secured manner.

Use Case 13c	Inquiry on a specific suspicious vessel (crew and ownership related)

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	ship, passenger, crew list, ownership, voyage, suspected person, position, cargo, known criminal background on person on board + historical datas (ship, crew list, voyage, position)	Intelligence report: anomaly, risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	collection of intelligence and field reports	will ask for other analysis from other intelligence provides	
analyse further info	Analyst	collection of intelligence and field reports	analysis report: consolidated intelligence report, recommendation		
provide further info	Intelligence provider	RFI: sighting, VHF contact, etc…	RFI reply	provide information from the field	
decide COA	Operations decision maker	analysis report	selected course of action		
update intelligence	Intelligence provider				
forward info	Operations decision	analysis report and	action request or notification		

Activity	Role	Input	Output	Description/example	New entities
	maker	selected course of action	(including the analysis report and selected course of action)		
issue operational instruction	Operations decision maker	analysis report, available assets, other operations in the area	set of operational instructions (how, who, when, why, where, what)		
Action	Operations decision maker	set of operational instructions	set of operational instructions (how, who, when, why, where, what)		
close operation	Operations decision maker	several situation reports	after action report		
update intelligence on closure	Intelligence provider				

List of services for the activity "analyse available information"

Service type	Name	Operation	Input	Output	Pattern	description
Task service	**Same as 13 b**					
Support service	**Same as 13 b**					
Entity service	Passenger service		Passenger personal data (name, first name, date of birth, nationality for ex.)	Passengers of interest suspected of breaking the law	Pull	Ability to target suspected persons located on a vessel
Entity service	Crew list service		Crew list personal data (name, first name,	Persons of interest suspected of breaking the law	Pull	Ability to target suspected persons located on a vessel

Service type	Name	Operation	Input	Output	Pattern	description
			date of birth, nationality for ex.)			

Use Case 25b	Investigation of antipollution situation(law enforcement)

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	ship, pollution event, satellite images, aerial photo, volontary pollution report	Intelligence report: anomaly (potential pollution), risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	analysis report: consolidated intelligence report, recommendation (including for instance POLREP)	will ask for other analysis from other intelligence provides	
decide COA	Operations decision maker	analysis report	selected course of action		
forward information to partner	Operations decision maker	analysis report and selected course of action	Intelligence report		
Request action from partner	Operations decision maker	analysis report and selected course of action	Action request		
issue operational instruction	Operations decision maker	analysis report, available assets, other operations in the area	set of operational instructions (how, who, when, why, where, what)		

Activity	Role	Input	Output	Description/example	New entities
Act and provide feed back	Executor	set of operational instructions	Situation report		
close operation	Operations decision maker	several situation reports	after action report		

List of services for the activity "analyse available information"

Service type	Name	Input	Output	Pattern	description
Task service	Antipollution investigation	Ship, ship history, Area, Cargo, crew, owner,	Report on ship, ownership and cargo.	Push pull	
Support service	- databases - planning tools - drift models	voyage data, hazardous materials, natura 2000, wild life, protected areas, drift models,		pull	
Entity service	- various ship data related	VMS, AIS, LRIT, radar track, clean sea net		pull	

Use Case 44	Request for any information confirming the identification, position and activity of a vessel of interest

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	tracks (including sighting), history of tracks, voyage, history of voyage, port movements, ship, ownership, crew passenger	Intelligence report: anomaly, risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	analysis report: consolidated intelligence report, recommendation	will ask for other analysis from other intelligence provides	
decide COA	Operations decision maker	analysis report	selected course of action		
forward information to partner	Operations decision maker	analysis report and selected course of action	Intelligence report		
Request action from partner	Operations decision maker	analysis report and selected course of action	Action request		
issue operational instruction	Operations decision maker	analysis report, available assets, other operations in	set of operational instructions (how, who, when, why,		

Activity	Role	Input	Output	Description/example	New entities
		the area	where, what)		
Act and provide feed back	Executor	set of operational instructions	Situation report		
close operation	Operations decision maker	several situation reports	after action report		

List of services for the activity "analyse available information"

Service type	Name	Input	Output	Pattern	description
Task service	Confirmation of a vessel ID, POS and activity	Ship id Area Position Activity	Confirmed (updated) requested vessel data report	Push	
Support service	Validation, fusion, correlation	Vessel ID	Correlated, fused information on ship, voage, crew, passengers, port history, area	Pull/ pull delayed	
Entity service		Ship data Voyage data Crew Passenger Cargo Port history data Area	Vessel information	Pull/ pull delayed	

Use Case 57	Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance (Baseline and Targeted operations)

List of activities

Activity	Role	Input	Output	Description/example	New entities
1. Fill in the surveillance gaps. Need for enhancing or complement surveillance in areas where surveillance is poor or there is a specific surveillance need.	- Analyst - Operations decision maker - Operations executor	surveillance capacity filling the gaps	Better surveillance in he identified gap areas	to plan mission at sea	
2. Sharing of the costs	Operations decision makers				
3. Roster of the activities and assets					
4. Extra resources to fill in the gaps	- Operations decision maker	Level of readiness of resources in the countries and EU organizations			
5. Sea basing cooperation using the territorial waters etc			Agreement of using the national territorial areas of the regional countries		

List of services for the activity "Retrieve surveillance capacities"

Service type	Name	Input	Output	Pattern	description
Task service	-Enhance the surveillance capability - enhance the transparency - create the culture of cooperation	- Information from defined area - Information of a particular contact of interest	Surveillance plan - Available surveillance resources - Roosters of activities - Knowledge of surveillance gaps (not covered 24/7 or at all without moving the assets)	All	
Support service	- Detection - Identification - Tracking - Enrichment				
Entity service	Detection - Radar - visual sightings - electro optsics - geospatial services - sifgint etc Identfication - ISAR				

Service type	Name	Input	Output	Pattern	description
	- Human sightings - AIS - LRIT - SafeSea net etc - Electro optocs - radar - sonar / hydrofones Tracking - ISAR - Human sightings - AIS - LRIT - Safe Sea Net etc - Radar - Sonar / Hydrofones - Anomaly detection Enrichment - Contact information Support Cooperative tools - Communications - Analyses tool				

Use Case 70	Suspect Fishing vessel/ small boat is cooperating with other type of vessels (m/v, Container vessel etc.)

1 Changes from expected data/particulars related to vessels is important

2 Definitions and some language needs checking for accuracy to ensure a common understanding

3 Known risk factors within each/every community is needed and this is separate from operational risk assessment

4 Some over-arching concerns of data protection and governance issues

5 Do not close traditional networking techniques but manage with governance

List of activities

Activity	**Role**	**Input**	**Output**	**Description/example**	New entities
analyse available information	Intelligence provider	track, track history, fishing vessel, vessels data, voyage, voyage history, cargo, ownership, crew, passenger, port movements, last inspection reports, caches, licences	Intelligence report: anomaly, risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	analysis report: consolidated intelligence report, recommendation	will ask for other analysis from other intelligence provides	
decide COA	Operations decision maker	analysis report	selected course of action		
forward information to partner	Operations decision maker	analysis report and selected course of action	Intelligence report		

Activity	Role	Input	Output	Description/example	New entities
Request action from partner	Operations decision maker	analysis report and selected course of action	Action request		
issue operational instruction	Operations decision maker	analysis report, available assets, other operations in the area	set of operational instructions (how, who, when, why, where, what)		
Act and provide feed back	Executor	set of operational instructions	Situation report		
close operation	Operations decision maker	several situation reports	after action report		

List of services for the activity "analyse available information"

Service type	Name	Input	Output	Pattern	description
Task service	detection of vessels cooperating at sea for illegal activities	Area Time vector	Intelligence report	Pull delayed	Periodically provides an intel report with the list and location of vessels within the area of interest
Support service	IdentifiedI vessels and illegal activities	Area Time period		Pull	Returns the list of vessels and illegal activities
Entity service	Automatic tracks (AIS, VMS, LRIT, radar, satellite, CCTV), satellite) Manual tracks (sightings)	Area Time period Vessels	Intelligence report	Pull	Retrieves the known vessels within a specified area of interest reported by automatic

Service type	Name	Input	Output	Pattern	description
	Intelligence Ship details (owner, characteristics) Inspection reports at sea and land Cargo Crew – list, identification, criminal register, qualifications Goods Gears Track history Risk factor (black lists)				systems or manually by operators

Use Case 85	Anti-Piracy Maritime Surveillance and free navigation control: Merchant vessels at sea (outside Territorial waters) sends an alert that it is under Piracy attack

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	piracy alert	Intelligence report: anomaly, risk		
collect and analyse further info	Analyst	several intelligence report: anomaly, risk	analysis report: consolidated intelligence report, recommendation	will ask for other analysis from other intelligence provides	
decide COA	Operations decision maker	analysis report	selected course of action		
forward relevant information	Operations decision maker	analysis report and selected course of action	Intelligence report		
Request action from partner	Operations decision maker	analysis report and selected course of action	Action request		
issue of operational instruction	Operations decision maker	analysis report, available assets, other operations in the area	set of operational instructions (how, who, when, why, where, what)		
Act and provide feed back	Executor	set of operational instructions	Situation report		
close operation	Operations decision maker	several situation reports	after action report		

List of services for the activity "analyse available information"

Service type	Name	Input	Output	Pattern	description
Task service	There is ship under a piracy attack	- Alert - warning - anomaly detection - Common operational procedures	Support of the operation in the field: - communication - decision making - historical data and lessons learned from previous attacks - analyses report	All	
Support service	Available data, Loyds, history of the ship and its activities from various sources, piracy activities, lessons learned				
Entity service	Detection - Radar - visual sightings - electro optsics - geospatial services - sifgint etc Identfication - ISAR - Human sightings - AIS - LRIT - SafeSea net etc - Electro optocs - radar - sonar / hydrofones				

Service type	Name	Input	Output	Pattern	description
	Tracking - ISAR - Human sightings - AIS - LRIT - Safe Sea Net etc - Radar - Sonar / Hydrofones - Anomaly detection Enrichment - Contact information Support Cooperative tools - Communications - Analyses tool				

Use Case 93	Detection and behaviour monitoring of IUU listed vessels

List of activities

Activity	Role	Input	Output	Description/example	New entities
analyse available information	Intelligence provider	vessel, IUU list, port movements	Intelligence report: anomaly, risk		

List of services for the activity "analyse available information"

Service type	**Name**	**Input**	**Output**	**Pattern**	**description**
Task service	IUUVesselDetectionAndMonitoring	Area	IUU intelligence report (inc. area, position, vessel, activity, photo…)	pull delayed	Periodically provides an intel report with the list and location of identified IUU vessels within the area of interest specified
Support service	IdentifiedIUUVessels	Area	IUU vessels	Pull	Provides the list of identified IUU vessels within the area of interest specified, by matching the IUU vessels list with the RMP and Port movements information
Entity service	IUUVessels	No	IUU vessels	Pull	Returns the up to date list of IUU vessels
Entity service	AutomaticTracks	Area	Vessels	Pull	Retrieves the known vessels within a specified area of interest reported by autonatic systems such

Service type	Name	Input	Output	Pattern	description
					as AIS, LRIT or VMS
Entity service	ManualTracks	Area	Vessels	Pull	Retrieves the vessels within a specified area of interest reported manually by operators (i.e. sightings)
Entity service	PortMovements	Area	Vessels	Pull	Retrieves the vessels that are in ports within a specified area of interest

Annex V – List of Purposes

List of purposes for information sharing

References:

A. High-Level Use Cases

B. Events describing High-Level Services

C. Use Cases

D. List of Services

E. Data Matrix

Using the above references A-E, this list aims to describe which user community needs to share what information why and when. The list is not exhaustive, and do not describe all thinkable situations, but represent the situation in the use cases, which should be representing a good portion of the maritime information sharing environment.

Sector	Purpose	Use Case	Data (from data matrix)	
Maritime Safety, Security and prevention of pollution	Vessel traffic management			
	Vessel Traffic Safety			
	Monitoring of security of ships			
	Search and Rescue			
	Support of response and enforcement operations (anti-piracy, SAR, salvage)			
Fisheries Control	Early warning of illegal fisheries or fish landings,			
	Monitoring of			

	compliance with regulations on fisheries			
	Support of response and enforcement operations			
Marine pollution preparedness and response	Monitoring of compliance with regulations			
	Early warning of environmental accidents and incidents			
	Support of pollution response operations			
Customs	Monitoring of compliance with customs regulation on import, export and movement of goods			
	Support of enforcement operations			
Border Control	Monitoring of compliance with regulations on immigration and border control crossings			
	Support of enforcement operations			
General Law Enforcement	Monitoring of compliance with applicable legislation in sea areas where police competence is required			

	Support to enforcement and response operations			
Defence	Monitoring in support of defence tasks such as national sovereignty at sea			
	Combatting terrorism and other hostile activities outside the EU			
	Other CSDP tasks as defined in Articles 42 and 43 TEU			