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 4:

Definition of access rights

Co-Financed under European Integrated Maritime Policy

Table of Contents

1 Executive Summary 4
2 Background 4
2.1 Assigned Tasks and Their Expected Outputs 4
2.2 Objectives 5
2.3 Previous experiences 5
2.4 Levels of protection of information (classification) 6
3 The process 7
3.1 Inputs 7
3.2 Identifying the provider and customer 7
3.3 Assessing access rights 8
3.4 Information Services Pattern 9
3.5 Information Services Classification 9
4 Access rights matrixes 9
4.1 Service related to use case 13b 9
4.2 Service related to use case 13c 10
4.3 Service related to use case 25 10
4.4 Service related to use case 44 11
4.5 Service related to use case 57 11
4.6 Service related to use case 70 12
4.7 Service related to use case 85 12
4.8 Service related to use case 93 13
5 Access to input data 13
6 Discussion 14
6.1 Limitations to the “information services” 14
6.2 The TAG data matrix: the first building block of interoperability 15
6.3 Evolution of the landscape 16
6.4 Information classification 16
6.5 Personal data 17
6.6 Cooperation with third parties 18

6.7 Potential for CISE 18
6.8 Global Surveillance (white picture) 18
7 Conclusions 20
8 Recommendations 21
8.1 Increase the interoperability between authorities 21
8.2 Withdraw the obstacles to exchange of information 21
8.3 Encourage information exchange 22
8.4 Discover unknown areas 22
Annexes 23
Annex I – List of Acronyms and Abbreviations 24
Annex II – Meetings Summary 26
Annex III – List of legislation related to data exchange 27
Annex IV – Glossary 29
Annex V – Access Rights Matrixes 34
Annex VI – Illustration of information classification 45
Annex VII – Extract from BMM and MARSUNO experiences 46
Annex VIII – Output classification with regards to personal data 56
Annex IX – Purposes versus Use Cases 57
Annex X – Reminder for studies of access rights within the Use Cases 58
Annex XI – Coverage of TAG data matrix 60
Annex XII – Classification of information services / EU classification levels 61
Annex XIII – List of possible observed deficiencies of access rights and lack of needed information 62

1 Executive Summary

This report contributes the Test Project on Cooperation in Execution of Various Maritime Functionalities at Sub-regional or Sea-basin Level in the Field of Integrated Maritime Surveillance (later called CoopP, Cooperation Project or Project). It presents the results achieved in working package 4 which focused on the definition of access rights to maritime information.

Based on the results obtained by working package 2 on the definition of information services, working package 4 processed the information in order to assess what are the appropriate levels of access to information. For each use case working package 4 produces a generic access rights matrix, evaluates the level of classification of the services and identifies some deficiencies to be overcome in order to develop the exchange of information between authorities.

The works emphasized the upmost importance of the definition of the service. This service must be feasible, consistent, and adds value for the customers. The working package encourages further studies in this area.

The eight matrixes show the potential of a functional CISE in EU. With the exception of the current communication channels, the matrixes also identify exchange of information streams that cannot be exchanged currently because of a lack of organization and of technical means.

Working package 4 identifies ways to deal with the inherent complexity of the project. Current impediments to information exchange should not be under evaluated and organizational interoperability must be considered firstly before the legal and technical issues can be considered in development of CISE.

2 Background

2.1 Assigned Tasks and Their Expected Outputs

The Work Package 4 was assigned the following tasks:

- Establishing a generic access right matrix for each information service defined. Such matrix should detail conditions of access to information services based on the agreed list of purposes;

- Classifying the information services possibly with reference to the EU classification levels.

Access rights have to be studied on the basis of the WP2 results: list of description and definition of purposes. Access rights have to be based on juridical status, official tasks and purposes of authorities involved concerning information services.

The Work Package 4 had to investigate access rights using lessons learnt from previous pilot projects (MARSUNO, BMM and BSMF).

The above mentioned tasks were expected to be accomplished with following outputs:

Expected Outputs	**Output reached: yes/no; reference chapter/annex for results discussion**
Generic access rights matrix per information service.	Yes, see chapter 4 and Annex V
Classifying the information services possibly with reference to the EU classification levels.	Yes, see chapters 3.4 & 6.3 and annex XII
List of possible deficiencies of access rights and lack of needed information	Yes, see chapter 6 and annex XIII

2.2 Objectives

The Cooperation Project is expected to reach 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)

From these objectives, the Objective 1 falls partly under the responsibility of WP 4.

A table of predefined Output and Result Indicators is presented in Annex II with a summary of delivered outputs and results.

2.3 Previous experiences

The previous pilot projects MARSUNO, BMM, and BSMF studied the questions of data protection and access rights. All these projects used the same categories of protection of data. The main conclusion of these projects concerns availability of data and personal data protection.

All project concluded that most of the data could be considered as “basic data” and then could be shared easily. For example, basic data are tracking information originated from sensors, observations, position, speed, length of a ship, etc. There are therefore technical issues to manage the exchange of high amount of data within numerous actors.

The protection of personal data is at the source of one of the biggest constraints in data management. Personal data is not to be processed for purposes other than those for which they were collected. The personal data must be, at first, identified. Then, the purpose must be known and legitimate before an actor can have access to this data.

An extract from BMM and MARSUNO experiences is in annex VII.

2.4 Levels of protection of information (classification)

Two classification scales of information protection exist in the landscape.

The first comes from the official security rules of European Union and relates to national security. Its four levels of classification of information (EU restricted, confidential, secret, top secret) are defined in relation to the essential interests of the European Union.

The second classification has been used by all the previous projects. It divides information into three categories: basic data, additional data and restricted data. Only the third category concerns sensitive information. The two others categories do not deal with sensitive information and use open source information. Basic information can be freely exchanged inside the CISE community, and additional information can be shared on user demand.

See the comparison of the two scales in annex VI.

The EU restricted level does not correspond exactly to the restricted data categories. The restricted category has a broader scope including some levels of EU classification, but also commercial sensitive information, not relevence to the EU interests. Other sensitive information is information considered as ”personal data”[1].

Among all data sets described in the TAG data matrix[2], only a limited number of data are EU classified. For example, information related to a possible terrorist threat could be classified “EU confidential” (see category C.6.3. in the TAG data matrix). The counter-terrorism intelligence was not included in the use cases studied. Among the use case, very few output information could be considered to have a level of classification above “restricted”.

[1] Personal data are sensitive information, but generally are not classified information.
[2] The TAG data matrix has been elaborated by experts. It has no specific legal basis. The classification of information is made by the competent authorities.

3 The process

3.1 Inputs

Acces rights have to be studied on the basis of the Working Package 2 results. The main results are the information services developed from the eight uses cases studied by Working Package 2.

Working Package 4 considered, in addition, the reports of MARSUNO, BMM and BSMF projects, where the access right issues have been identified. These former pilot projects studied these access rights issues from a broad perspective. The cooperation project however focused on specific examples i.e. the eight uses cases as presented. So the questions asked to Working Package 4 are more pragmatic and case specific.

Working Package 4 processed the information services described in the document “List of services v 3.0.docx”. With reference to the methodology used by working packages 2 and 5, and guidances of its leaders, Working Package 4 considered the “task services”, defined as “services that implement a business function” as the information services. Support services and entity services are lower level services used to produce the task service.

3.2 Identifying the provider and customer

When referring to services, it appears obvious that a service is an interaction between a provider and a customer. In a broad view, all information exchanges between public actors could be seen as services provided to customers. The notions of “provider”, “services”, “customer” refers to a business model. It is necessary to describe this model, in order to develop a services oriented architecture (SOA) information system.

Identifying the provider and customers of the services was an activity of the upmost importance within the Working Package 4 tasks. In most of the use cases, the provider can not be a member of any of seven communities[3]. The services must correspond to the mission and the public actor seen as the provider. The customer must be a legitimate customer and the request must be of pertinence to the customers needs.

[3] For example, in the use case 13c, the provider can not be a public actor of the fisheries or marine pollution communities.

Excluded from the scope of the project are:

- Exchanges within one member state (provider and customer in the same member state)[4],
- Exchange with a third state (provider or customer in a state outside European Union and European Economic Area)[5],
- Exchanges between a public actor and a private actor,
- Exchange with an intelligence agency.

3.3 Assessing access rights

Access rights are defined through a multicriteria process using Working Package 2 material and Working Package 4 member's experiences.

The definition of the service, the output and the pattern are extracted from the list of services; table list of services for the activity; line "task service", columns "name", "output" and "pattern". The sensitivity of the output is assessed by Working Package 4 members. The output is linked with one or several data set(s) of the TAG data matrix.

For the providers and customers, different examples are developed by Working Package 4. The four generic examples are in the following table.

provider	**customer**
Member state public actor	Member state public actor
Member state public actor	EU agency
EU agency	Member state public actor
EU agency	EU agency

The purpose is underlying in the use case. A table of correspondance between the purposes and the uses cases has been elaborated by the Working Package 2. Some of the eight use cases covers different kinds of purposes (see annex IX).

Three levels of access rights have been used:

- F : Full access
- C : on a Case by case basis

[4] CISE is consistent with the principle of subsidiarity.
[5] CISE concerns interoperability in the European Union (and EEA).

- N : No access, or NR for “not relevant”

The letter in the matrix represents the level of access wanted. If the current access level is different, two letters are set in the matrix. The first represents the present situation and the second, the desired situation, needing some official text changes.

3.4 Information Services Pattern

The pattern of the information service describes the process linking the provider and the customer of the service. Four main types of pattern are considered:

Pull: the consumer knows the exact provider and asks for the Information which is immediately made available (synchronous).

Pull delayed: the consumer knows the exact provider and asks for the information which is made available only if and when possible (asynchronous).

Broadcast pull: the consumer does not know the exact provider and asks for the information to all the possible providers. The information is made available only if and when possible (asynchronous). Several responses may occur.

Broadcast push: the provider does not know who is willing to consume, therefore it broadcasts the information to all possible consumers (synchronous).

3.5 Information Services Classification

The classification is studied for each use case. The sensitivity of the different output is assessed. Annex XII shows a synthesis of these evaluations.

4 Access rights matrixes

This chaper describes briefly the eight use cases. These matrixes are in the annex V.

4.1 Service related to use case 13b

Inquiry on a specific suspicious vessel (cargo related)

The service provided is the targeting of illegal cargo vessel. The outputs are an intelligence report and additional data for further risk analysis. The pattern, “broadcast push” is the case where a provider sends the information to several actors.

In that specific use case, the provider of the service is likely to be in the customs or in general law enforcement communities. Contribution of other communities are not excluded, but with a low probability of occurrence. The customers having full access rights in this instance are in the customs and general law enforcement communities. So, the pattern defined by the working package 2 seems not to fit to the access right matrix. From the working package 4 opinion, the appropriated pattern is a “pull” or “pull delayed”.

4.2 Service related to use case 13c

Inquiry on a specific suspicious vessel (crew and ownership related)

The service provided is the targeting of suspicious vessel. The outputs are an intelligence report and additional data for further risk analysis. The pattern, “broadcast push” is the case where a provider sends the information to several actors.

In that specific use case, the pattern defined by working package 2 had raised questions. As far as suspicious activities of specific persons are identified, the level of sensitivity is high and the information can not be broadcasted. The risk is more likely to a failure in a law enforcement operation than a threat to EU essential interest, but it is not excluded. Working Package 4 considered then a pattern “pull” or “pull delayed” (communication to identified customers) to be the appropriate pattern in this instance.

4.3 Service related to use case 25

Investigation of antipollution situation (law enforcement)

The service provided is an antipollution investigation. The output is a report on ship, ownership and cargo. The pattern, “pull” is the case where a provider sends the information

to others authorities on demand. The process is generally a push, since the process from detection to law enforcement is well known.

4.4 Service related to use case 44

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

The service provided is a confirmation of a vessel ID, POS and activity. The output is a report on confirmed (updated) data concerning the requested vessel. The pattern, “push” is the case where a provider sends the information to several actors. WP4 adopted a pattern “pull delayed” which seems to be better adapted to the use case. The outputs are a set of data element, all considered as basic data or at least additional data. None are restricted. None are “personal data” with the provision of not containing element usable to identify a person.

4.5 Service related to use case 57

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

The service allows the enhancement of surveillance capability. The outputs are information useful to elaborate a surveillance plan (resources, list of activities, gaps). The prefered pattern is “pull delayed”. The customer is likely to plan surveillance in the area of responsibility of its own state. The given sea areas could be the EEZ or SRR (more likely in a neighbouring area) of a member state or in high sea (probably in a targeted operation). The customer could be another member state or an agency. The service is considered to be the communication of assets availability to a customer which is in charge to plan the surveillance in its area of responsibility. The outputs are information concerning the assets (characteristics, position, and contact). The information can be restricted (position of the asset). Personal data must not be an issue (contact information could be anonymous, if not, no limitation to share the name of point of contact between public actors).

Two access rights matrix have been elaborated to reflect the two different situations: baseline or targeted operations. Several lines are used to take into account the diversity of the possible operations.

4.6 Service related to use case 70

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

The service provided is the detection of vessels cooperating at sea for illegal activities. The output is an intelligence report. The pattern, “pull delayed” is the case where a customer is requesting the service to a provider that has a relevant surveillance activity. The provider can send the report to the customer each time a suspected behaviour is detected.

Some public actors are more likely to be able to provide this service. For that, the public actors must own non cooperative sensors, and especially mobiles sensors (patrol vessels, surveillance aircrafts, long range radar …). In the real life, the vessels of attention are likely to be detected in the area of responsibility of a member state that will conduct further investigations. The provider could however need information from another public authority in EU (input data). It is assumed that an authority is not developing a service out of the scope of its missions.

The customer must be legitimated (has the right to get a “purpose related information”). In use case 70, the provider could be a law enforcement authority (Border control, customs, general law enforcement), or Fisheries authorities in the case where a fishing vessel may be involved.

A specific line in the matrix deals with an example illustrating the EMSA / FRONTEX cooperation agreement. Most of the participants considered the case not relevant.

4.7 Service related to use case 85

A merchant vessel at sea (outside Territorial waters) sends an alert that it is under Piracy attack.

The objective of the process is to support the operation. The scope of the operation has been discussed during the meetings and the conclusion was to distinguish two different responses:

- a limited operation restricted to the recovery of the attacked ship,
- a more global operation including for example measures to prevent other attacks.

The service provided is the communication of all data element concerning the case. The customer prepares element to support the operation and is requesting information from differents providers. The pattern in this case is “pull”. Some data elements could be considered as EU confidential. The customer is more likely to be of the flag state, the state of the ship owner or the state that have national citizens on the attacked ship. The customer could need other information as cooperative or non cooperative position data. In this case, it could request an information service relating to Use Case 44. It is more likely to need non cooperative data from additional sources i.e. a space agency (for example EUSC).

4.8 Service related to use case 93

Detection and behaviour monitoring of IUU listed vessels

The information service is to provide data elements to a customer in charge of an IUU intelligence report. The customers are requiring information concerning IUU vessels in order to elaborate the report.

5 Access to input data

“Input data” is the information that the provider needs to hold in order to elaborate the service. A legitimated provider is acting in accordance to its missions and disposes of adapted means to collect the information. It could have a complementary need and then could become a customer of an information exchange. It is difficult to assess the need of complementary information, since it depends on the specific case. Input data is, as a consequence, dealt with a different process from the output data.

“Input data” is picked up in the list of services; table list of activities; line “analyse available information”, columns “input”.

Data often belongs to its creator. To identify exactly access rights to the data, the reasons why this information is requested must be analyzed. This information can come from:

- Registers
- Ships or shipping companies,
- National public sensors,
- Multinational public sensors,
- Commercial/private sensors/services.

The analyses must also take into account the fact that the data could be turned into different data sets - for example primary data merging with others data sources and analysis to produce new information.

The flag State is, in some cases, an important actor to be considered (for example in Vessel Monitoring System for fishing vessels).

Further studies in this area needs to be undertaken in any future CISE projects.

6 Discussion

6.1 Limitations to the "information services"

The cooperation project is focused on very limited use cases. The cooperation project is broader than the former pilot projects "Marsuno" and "BMM" from a participation and geographical scope points of view, but narrower from an exchange of information point of view.

The use cases are focusing on illegal activities and, as a consequence, the exchange of information generally takes place between law enforcement authorities. A large part of the services studied develops intelligence reports (data corresponding to table C of the TAG data matrix) that must be considered as "restricted". Very few higher levels of classification have been noted. Considering input information, the volume of data elements considered is high. But the part of data elements produced by the provider itself has not been identified. It is assumed that the provider of the service is the public authority that has the means to produce the main data elements. It could need additional data elements to produce a

higher quality service, but it could provide a service on its own. This quality level of the service has not been assessed.

It must be understood that when the output of a service is an intelligence report, there is no link with reports produced by intelligence agencies.

The ability to provide a service depends on different kind of information:

- Four services can be provided by using surveillance sensors or opportunity sources (25, 44, 70, 93),
- Two services need an external intelligence source (13b & 13c), with restricted material,
- One needs the knowledge of the actors capabilities (57),
- The last (85) needs different kinds of information and occurs in waters outside the EU.

This difference between the use cases must be taken into account in the study of the solutions of information exchange. Particularly, it deserves to assess the best answer between a unique solution of different kind of answers.

6.2 The TAG data matrix: the first building block of interoperability

When assessing access right for maritime information, the TAG data matrix emerged as a key element during discussions within the working package 4. It was also a shared element with the other working packages. It eased considerably the discussions and allowed to fix some difficulties.

It was possible to assess the sensitivity of information of each data element involved in the eight use cases. The level of classification was easier to estimate and the question of the personal data easier to handle.

Some improvements to the TAG data matrix could be made, particularly, concerning the following data elements:

- A.3.3.1.1. “ship photograph”: must be considered in this data element only photograph without element allowing the identification of a person.
- A.2.1.7 “activity”: the data element deserves to be illustrated,
- A.3.2.1.7. “IMO number”: the data element must be named “IMO ship number”.

6.3 Evolution of the landscape

The sectorial landscape has evolved in the last four years. Information systems have been developed and regulations have evolved.

Three European projects illustrate this evolution which seems to accelerate:

- The regulation Establishing the European Border Surveillance System (EUROSUR), adopted in November 2013,
- The revision of Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system,
- The directive 2010/65/EU on Reporting formalities for ships, establishing National Single Windows.

6.4 Information classification

From the discussions, it seems that all public actors are not using a classification level similar to those of EU. Although the question of the classification is not central in the study of the use cases, it would be interesting, in future studies, to compare the methods of protection of the information of the concerned public actors.

In the eight use cases, the level of classification of the output has been evaluated as “restricted”. Only one data element in one of the use cases seems to need a greater level of classification. The protection of industrial or commercial confidentiality is considered to be guaranteed by the level “restricted”. It must then be considered that the level of protection of the information systems must be restricted.

Currently, most of the systems can not handle restricted information. SIENA is an example of a network able to exchange restricted information. SIENA not only links MS Europols national units, but also other competent authorities.

6.5 Personal data

Among some hundred of data sets, IMO ship number[6] is a key element[7] for exchanging information between public actors. When discussing personal data, the status of IMO ship number appears unclear. Although considered non personal data for most of actors, the IMO ship number is considered by some partners to a certain extent as a personal data that could cause a limitation to exchange and use of the data. To avoid a restrictive different interpretation by different actors, it would be advisable to seek the opinion of the European Data Protection Supervisor on the question of whether and under what conditions an exchange of vessel traffic information is permissible in the light of the data protection law. To ease information exchange, it would be desirable that the status “no personal data” of IMO ship numbers would be stated in an EU legally binding text, and by extension to other data elements describing a “vessel”. It is of the upmost importance to have consistency between all sectoral legally binding texts[8].

A picture of a ship where a person could be identified is considered as a personal data. To avoid a legal uncertainty, it is recommended that all “Ship photograph”, entering in the data element A.3.3.1.1, must not contain elements allowing identifying a person. The TAG data matrix could be updated to take this consideration into account. It would be possible, for instance, to create a new data element “person aboard a ship” in A.2.3.

The TAG data element A.3.2 “Ship ownership and operation data” generally does not include any personal data. But one element, A.3.2.1.5 “ship owner” could be personal data if the owner is a natural person and not a company.

In the eight use cases, the output does not include personal data information in any obvious manner. In one of the use cases, the outputs include personal data (UC 13c). In four others, the ouputs could include personal data (13b, 25, 44 & 93). In three remainders, the outputs do not normally contain personal data. In any case, in these use cases, the protection of personal data is not an obstacle for sending the information to the legitimated customer.

[6] International Maritime Organization (IMO) numbers are unique identifiers for ships, introduced under the SOLAS Convention to improve maritime safety and security and to reduce maritime fraud.
[7] The MMSI Number and the name of the ship are also used to identify a ship .
[8] The new EUROSUR regulation mention IMO numbers in a article concerning the protection of personal data (art 13)

The maritime public actors should be encouraged to be compliant with data protection rules. Provisions are already contained in some documents (DIRECTIVE 2009/17/EC)[9].

6.6 Cooperation with third parties

Some partners have reported examples of automatic exchange of data with other partners in a regional basin. Some basin fora include information sharing with third parties. This action must be assessed precisely when the data bases contain EU restricted information.

Nevertheless, cooperation with third parties represents an opportunity of gathering more information concerning European areas of interest. Cooperation with third state and international organization must be encouraged.

6.7 Potential for CISE

Discussions on the matrixes have focused on what must happen. Sometimes, the present situation does not represent the desired situation. So the matrixes identify clearly the potential for CISE, from the access rights point of view. More over, it is possible to assess if there is a direct communication channel to allow the exchange of information. In most of the cases, this does not exist, which undermines CISE.

Some use cases present a bigger potential for CISE, especially when the data exchanged is not classified, and when there are lots of possible customers. The use case 44 is an illustration of this potential. In other use case, the potential lies more in a regional level, as in use case 57.

Beyond the questions of access right, the flow and the volume of the data exchanged needs hightlighting as its poses technical challenges.

6.8 Global Surveillance (white picture)

[9] Art 24 : Member States shall, in accordance with Community or national legislation, take the necessary measures to ensure the confidentiality of information sent to them pursuant to this Directive, and shall only use such information in compliance with this Directive

Working package 4 has discussed also the concept of “White Picture”.

Information concerning ship, their position and route are basic data that would be advantageous to be shared more widely within Europe. But this basic data represents a huge amount of information. Today, there are 70 000 ships with a gross tonnage of 300 tonnes and this is expected to rise to over 120 000 vessels. With the addition of small crafts, AIS transmitting vessels could reach a figure of about 2 million. Getting accurate information of these ships is the first challenge. A second challenge is how to filter position and route of vessels of interest. This is a huge task with each AIS enabled vessel transmitting its position information about 10 000 times in a year.

The different purposes as per in annex IX require different ways ahead as far as frequency of data interchange on one hand and geographical range of data interchange on the other hand is considered. It is still unclear what practical value is the provision of such information in the whole EU-area. The near real life detection of traffic flows is only useful if traffic areas that are adjacent to each other are considered. In these cross-border activities, additional work may be required so as to ensure effective ship traffic data availability to relevant competent authorities. Current information sharing models in the Baltic Sea and North Sea illustrate the benefits of vessel information sharing between juristictions. Consideration should be given to the creation of regional CISE areas within the EU rather then on a single EU CISE region. This it is felt to be more cost effective and efficient way to deliver CISE. Each regional CISE should have the ability to transfer information to the other adjacent regional CISE areas.

Other purposes like "combating terrorism and other hostile activities outside the EU" will require a more comprehensive approach. For those purposes a balanced information exchange policy (type of information x exchange frequency) could be developed to support the respective purposes with a limited amount of information. In other cases and out out concrete situations as described before there is no necessity of sharing of all traffic data continuously within the whole EU.

As an exceptionless rule, CISE provides only interfaces. CISE is not a new system with its own databases and presentation tools.

7 Conclusions

The working package 4 on access rights has gathered up to thirty experts (end use, legal aspects, and information technology aspects). 23 public authorities of 10 member states and two European agencies have participated. All sea basins were represented.

All the use cases have been evaluated, and are concluded by an access right matrix. The classification levels have been assessed and some deficiencies have been identified.

The access right matrixes are generic in the sense that they don't deal with all possibles cases. Further analysis would need to go beyond the communities' level. The matrix represents only a shared expert's vision, without commitment of each authority.

The work was an opportunity to become aware of the complexity of CISE. A part of this complexity comes from the lack of similarity between the communities and the public authorities of each member state. Some public authorities have areas of responsibilities that are different from one member state to another.

The work emphasized the utmost importance of the definition of the service. This service must be feasible, consistent, and add value for the customers. A slight change of the definition of the service has sometimes been necessary.

The eight matrixes show the potential for functional CISE. With the exception of the current communication channels, the matrixes identify useful exchange of information not possible today because of a lack of organization and of technical means.

However, the difficulties must not be underevaluated when public authorities want to exchange classified information. Today, only the SIENA system from the law enforcement community allows the exchange of restricted information within European Union[10].

[10] Schengen channel (SIREN) and Interpol Channel can also be used by Law enforcement community.

8 Recommendations

The work allowed identifying actions likely to favor the construction of CISE. The recommendations stemming from the working package 4 are divided in four categories.

8.1 Increase the interoperability between authorities

- Develop the business process that includes information services and assess their value,
- Update the TAG data matrix and dictionary,
- Develop mutual confidence in the way personal data are handled,
- Develop a common understanding on the management of an IT system able to share EU restricted information

8.2 Withdraw the obstacles to exchange of information

- Reduce the "purpose restriction" of basic[11] information between authorities, especially in the VTM directive under revision,
- Reduce the number of data elements that could include personal data. For example :
    - exclude a ship picture when a person is identifiable (and create another data element for "person aboard a ship"),
    - study the possibility of clarifying the status of the IMO ship number to state[12] formally that the IMO ship number is not a personal data (as the name of the ship),
    - if not possible, study a purpose related legal base to enable the legitimate exchange and storage of personal data like IMO ship numbers or equivalent.

[11] Basic and non personal data.
[12] One partner feels that it is not possible.

8.3 Encourage information exchange

- Establish the mapping of current data flow in order to have a reference point,
- Implement CISE solutions in several steps,
- Recommend to exchange best practices,
- Recommend the automatic exchange of basic data in neighboring areas,
- Use the opportunity of current networks and initiatives (implementation of EUROSUR, MARSUR and IMDATE)

8.4 Discover unknown areas

- Provide relavant public authorities with more information :
    - Develop shared services using current assets,
    - Develop new assets to increase the coverage of surveillance,
- Develop cooperation with third States (at regional sea basin level but also at worldwide level, especially in piracy areas).

Annexes

Annex I - List of Acronyms and Abbreviations

Annex II - Meetings summary

Annex III - List of legislation related to data exchange

Annex IV - Glossary

Annex V - Access Rights Matrixes

Annex VI - Illustration of information classification

Annex VII - Extract from BMM experience

Annex VIII – Output classification with regards to personal data

Annex IX – Purposes versus Use Cases

Annex X – Reminder for studies of access rights within the Use Cases

Annex XI – Coverage of TAG data matrix

Annex XII – Classification of information services / EU classification levels

Annex XIII – List of possible observed deficiencies of access rights and lack of needed information

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
EEZ	Exclusive Economic Zone
EMODnet	the 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
EUSC	European Union Satellite Centre
FP7	EU Seventh Framework Programme for research and technological development
FRONTEX	the 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 Assesment
ID	Identity
IMDatE	Integrated Maritime Data Environment
IMO	International Maritime Organization
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations
IUU	illegal, unreported, unregulated
JRC	Joint Research Centre
LRIT	Long-Range Identification and Tracking of ships system
MARSUNO	Pilot Project: Maritime Surveillance North
MMSI	Maritime Mobile Service Identity
MSEsG	Member States Expert sub-Group

POV	Pre-Operational Validations
POS	Position
SafeSeaNet	Vessel traffic monitoring and information system
SAR	Search and Rescue
SRR	Search and rescue region
SEIS	Shared Environmental Information System
SIENA	Secure Information Exchange Network Application
SOA	Services oriented architecture
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 reaching of project objectives under the responsibility of WP 4 was measured with following output and result indicators. In the following table is a summary of the delivered outputs and results with a reference to more specified results.

Outputs are all the tangible results, milestones, and specific activities that were achieved, in order to complete the project. They directly result from the activities carried out in the project. They report on the main activities carried out during the project. They do not lead to a qualitative judgment on the project's outcomes.

In other words, it is not because the project organises a high number of workshops that it will necessarily be successful. Output indicators are typically measured in physical units such as the number of meetings, seminars, site visits, conferences, participants, publications.

Results are direct and immediate effects resulting from the project and from the production of the outputs. They do not report on the 'what' but on 'why' the project is delivering the specific outputs. The organization of interregional events and meetings, the identification and dissemination of good practices, etc. are only means to an end. These activities are carried out in order to achieve specific effects that the result indicators should be able to assess and measure in quantified terms. Therefore, compared to the outputs, they imply a qualitative value. They also have to be measured in physical units such as the number of staff with increased capacity, the number of good practices successfully transferred or the number of policies improved.

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 meeting (march, june, july, october) • 9 member states, around 21 partners • 20 to 28 participants
Results Indicators:	**Delivered Results:**
Access rights table for each information service defined. Target value corresponds to all necessary access rights attached to all information services defined.	• 8 draft matrixes
Classifying the information services possibly with reference to the EU classification levels.	• EU Restricted level mainly (in one case, could be confidential) • Classification of previus pilot projects still relevant

Annex III – List of legislation related to data exchange

1. United Nations Convention on the Law of the Sea (Montego Bay Convention 1982)
2. United Nations Convention against Transnational Organized Crime and the Protocols
3. Lisbon Treaty (13/12/2007)
4. Schengen acquis
5. Naples II Convention - Council Act f 18 December 1997, drawn up on the basis of Article K.3 of The Treaty on EU, on mutual assistance and cooperation between customs administrations
6. Council Framework Decision 2006/960/JHA, of 18 December 2006 - on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union said “Swedish initiative”
7. Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995 - on the protection of individuals with regard to the processing of personal data and on the free movement of such data
8. Directive 2002/59/EC of the European Parliament and of the Council, of 27 June 2002 - establishing a Community vessel traffic monitoring and information system (under revision) and repealing Council Directive 93/75/EEC
9. Directive 2003/4/EC of the European Parliament and of the Council, of 28 January 2003 - on public access to environmental information
10. Directive 2007/2/EC of the European Parliament and of the Council, of 14 March 2007 - establishing an Infrastructure for Spatial Information in the European Community
11. Council Framework Decision 2008/977/JHA, of 27 November 2008 - on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
12. Council Common Position 2005/69/JHA, of 24 January 2005 - on exchanging certain data with Interpol

13. Regulation (EC) n or 199/2008 of the Council regarding the establishment of a communitarian frame for the compilation, management and use of the data of the fishing sector settle down and the support to the scientific advising in relation to the common fishing policy

14. Regulation (EC) not 665/2008 of the Commission, of 14 of 2008 July, by which the dispositions of application of Regulation (EC) not 199/2008 of the Council regarding the establishment of a communitarian frame for the compilation, management and use of the data of the fishing sector settle down and the support to the scientific advising in relation to the common fishing policy

15. Regulation (EC) 1224/2009 of the Council, of 20 of November of 2009, by that a communitarian regime of control settles down to guarantee the fulfilment of the norms of the common fishing policy, Regulations (CE) 847/96 modify, (EC) 2371/2002, (EC) 811/2004, (EC) 768/2005, (EC) 2115/2005, (EC) 2166/2005, (EC) 388/2006, (EC) 509/2007, (EC) 676/2007, (EC) 1098/2007, (EC) 1300/2008 and (CE) 1342/2008 and derogate the Regulations (the EEC) 2847/93, (EC) 1627/94 and1966/2006 CE

16. Directive 2002/58/CE of the European Parliament and the Advice of 12 of July of 2002 relative to the personal data handling and the protection of the privacy in the sector of the electronics communications (relative Directive to the privacy and the electronics communications).

17. COMMISSION DECISION 2001/844/EC of 29 November 2001amending its internal Rules of Procedure “COMMISSION PROVISIONS ON SECURITY”

18. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

19. DIRECTIVE 2009/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 amending Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system

20. COM (2011) 873 final, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Establishing the European Border Surveillance System (EUROSUR)

21. Directive 2010/65/EU on reporting formalities for ships, establishing National Single Windows

Annex IV – Glossary

Glossary of terms for WP4 use

Access:

1. A means of approaching, entering, exiting, communicating with, or making use of: a store with easy access.

2. The ability or right to approach, enter, exit, communicate with, or make use of

Access control:

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system.

Access right (information technology):

Control the extent to which a particular user can use or edit a program or data file.

Aggregation (of information):

A function where requested information from multiple sources are grouped together to form a single response e.g. a list or a set.

Agreement:

A contract between one or more authorities acting as information providers and one or more authorities acting as information consumer to define the term and conditions for accessing and providing services. Can be bi-lateral (between 2 authorities) or community agreement (between more than 2 authorities). May include service level specifications in the form of Service Level Agreements (refer to SLAs).

Authority (or public authority):

Any organisation that has an interest in maritime surveillance information. An authority can be local, regional, national or European level.

Broadcasting:

A type of message distribution where a message is sent to all members, rather than specific members, of a group such as a department or enterprise.

Data:

Factual information, especially information organized for analysis or used to reason or make decisions.

Data controller:

The data controller is the person or administrative entity (for example a General Director or a Head of Unit of the European Commission) that determines the purposes and means of the processing of personal data on behalf of an institution or body. In particular, the controller has the duties of ensuring the quality of data and, in the case of the EU institutions and bodies, of notifying the processing operation to the data protection officer (DPO). In addition, the data controller is also responsible for the security measures protecting the data.

The controller is also the person or entity that receives a request from a data subject to exercise his or her rights. The controller must co-operate with the DPO, and may consult him or her for an opinion on any data protection related question.

Data mining:

Data mining is the process of analysing data from different perspectives and summarising it into useful new information. Data mining software is one of a number of tools for interrogating data. It allows users to analyse data from many different dimensions or angles, categorise it, and summarise the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery. Obviously, for data mining to be effective it is necessary to analyse large amounts of previously collected data.

Data protection authority:

A data protection authority is an independent body which is in charge of:

• monitoring the processing of personal data within its jurisdiction (country, region or international organization);

• providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data;

• hearing complaints lodged by citizens with regard to the protection of their data protection rights.

According to Article 28 of Directive 95/46/EC, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers (such as access to data, collection of information, etc.), effective powers of intervention (power to order the erasure of data, to impose a ban on a processing, etc.), and the power to start legal proceedings when data protection law has been violated.

Data protection officer:

Each Community institution and body shall, in order to comply with Regulation (EC) 45/2001, have a data protection officer (DPO). The DPO shall ensure the internal application of the Regulation and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations.

Duty:

is a term that conveys a sense of moral commitment to someone or something.

Information:

1. Knowledge derived from study, experience, or instruction.

2. Knowledge of specific events or situations that has been gathered or received by communication; intelligence or news. See Synonyms at knowledge.

3. A collection of facts or data.

Intellectual property (IP):

is a term referring to a number of distinct types of creations of the mind for which property rights are recognized—and the corresponding fields of law

Interoperability:

Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.

Large-scale IT systems:

Several databases (information systems) created or about to be created by the European Union (EU) can be considered large by various (sometimes all) measures: number of people using the system for different purposes, amount of data collected, stored, accessed, manipulated, number of connections between components, etc.

Notification:

a formal announcement

Obligation:

An obligation is a requirement to take some course of action, whether legal or moral.

Obstacle:

Synonyms: obstruction, bar1, barrier, block, hindrance, impediment, snag. All of these nouns refer to something that prevents action or slows progress.

Personal data:

Shall mean any information relating to an identified or identifiable natural person (“data subject”). A identifliable person is one who can be identified, directly or indirectly, in particulary reference to an identification number or to one or more factors specific to his physical, physiological, economic, cultural or social identity

Recipient:

Shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients

Request (or information request):

A message sent from an information consumer to an information provider, asking for information according to a certain criteria with the use of a common information exchange model.

Raw data:

unanalyzed data; data not yet subjected to analysis

Right, Rights:

In the jurisprudence and the law, a right is the legal or moral entitlement to do or refrain from doing something, or to obtain or refrain from obtaining an action, thing or recognition in civil society.

Secondary data:

Secondary data is data collected by someone other than the user.

Service:

Modular unit of business functionality that is made available through a service contract

Service contract:

Specifies all interactions between the service consumer and the service provider. This includes the service interface, interface documents, policies, QoS, performance

Task services:

Services that implement a business function

Use Case:

Within CISE context, use cases describe the circumstance of an operational situation for which there is a reason for a public authority to share or to request information with/to another public authority.

User community:

A user community is composed of a set of public authorities, which are bound together by their function e.g. customs, marine environment, maritime safety and security, defence, fisheries control, border control.

Annex V – Access Rights Matrixes

information service : Inquiry on a specific suspicious vessel (cargo related) (use case 13b)

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to Agencies	MS Customs or Law Enforcememt	C.6.2, C.6.5, A.2.2	C	C	C	no agency	C	F	no ops agency	EMSA.Limited to information concerning the purposes of safety (dangerous good, …) or risk of pollution, EFCA limited to fisheries purpose FRONTEX limited to border security ; EUROPOL no restriction from the identified providers
MS to MS	MS Customs or Law Enforcememt	C.6.2, C.6.5, A.2.2	C	C	C	F	C	F	C	Direct Link among Customs. No legal obligation to communicate. Limitation on the purpose for Maritime Safety, fisheries, marine pollution, border control.
Agency to Agency	Agency EUROPOL, EMSA	C.6.2, C.6.5	C	C	C	no agency	C	C / F	no ops agency	EMSA.Limited to information concerning the safety (dangerous good, …) or risk of pollution, FRONTEX limited to border security EUROPOL restriction because of the purpose (safety)
Agency to MS	Agency EUROPOL	C.6.2, C.6.5	C	C	C	F	C	F	C	available communication : SIENA : Direct link among LEAs & central system (EIS)
Agency to MS	Agency EMSA	A.2.2	F	C	F	C	C	C	C	"F" covered today : Direct link among maritime safety authorities. Limitation of purpose of safety
The provider of a report containing data elements A.2.2 can only be in the customs community. If not, the service is limited to more general information.										
The provider of this service is likely to be in the customs or in general law enforcement communities, but contributions of other communities are not excluded										

Information service :	Inquiry on specific suspicious vessel (crew and ownership related) use case 13c

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to MS	MS Customs Maritime Safety Border control	A.1.1, A.2.1, A.3, A.2.3.3, A.2.3.5, A.2.3.1, A.2.3.2	NR	NR	NR	NR	F	F	NR	A.1.1. and A.2.1 and A.3 : All basics data should be available to share. First it is out of the scope of CISE and second it will create a new data basis witch should be declared to the data protection authorities. A.2.3.3 (list of person on board) : no legal obstacle when info request on case by case basis by the customer using suedish initiative or Naple convention II. Europol may deliver additionnal information Schengen information system will be used to target list of persons on board. The reality of the purpose could be contested. A.2.3.5 (Intelligence on possible illegal cross border passager on board) :Frontex and Eurosur will provide these informations. It will be also usefull if the list of passanger is available to check Eurodac and VIS systems. A.2.3.1 (Master.Captain details) : judicial action if commercial data
MS to MS	MS Customs Maritime Safety Border control	A.3.2.1, A.3.2.3.18, C.8.2	NR	NR	NR	NR	C	C	NR	A.3.2.1 (Commercial ship ownership and operation data) : Commercials data could be protected by law and a european legislation will be necessary to get access to these categories of data. Need of a new legislation to obtain and share the data element from the private sector. A.3.2.3.18 (Element of suspicion elements of antecedents): Bicameral procedure CRI could be necessary to get antecedents of the persons on board.
MS to MS	MS defence authorities	C.6.3 Terrorist Threat	NR	NR	NR	NR	N?	C	C	It will be a difficult issue because in a majority of members states these kind of data and in particular the passager name records are not collected. Suedish initiative is not applicable to intelligences agencies. Defence is concerned when terrorist threat in relation to piracy
MS to Agency	MS PA	A.1.1, A.2.1, A.3, A.2.3.3, A.2.3.5, A.2.3.1, A.2.3.2	NR	NR	NR	NR	F	F	NR	
Agency to MS	Agency Europol, FRONTEX	A.1.1, A.2.1, A.3, A.2.3.3, A.2.3.5, A.2.3.1, A.2.3.2	NR	NR	NR	NR	F	F	NR	
Agency to Agency	Agency Europol, FRONTEX	A.1.1, A.2.1, A.3, A.2.3.3, A.2.3.5, A.2.3.1, A.2.3.2	NR	NR	NR	NR	F	F	NR	

Information service : to provide a set of data elements to the customer that has requested the data elements

information service : Investigation of antipollution situation (law enforcement) use case 25									
example	provider	Data element ref.	Customer (communities)						comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
agency to MS	Agency EMSA	A111, A21, A311, A331	F	NR	F	NR	NR	F	NR	info pushed by provider to several MS authorities> No legal obstacles. No other agency able to provide the service
MS to MS	MS PA, mainly Maritime Safety, but also Customs,	A111, A21, A311, A331	F	NR	F	NR	NR	F	NR	pattern usually "push" , but must be considered as a "pull" service
MS to Agency	MS PA, mainly Maritime Safety, but also Customs,	A111, A21, A311, A331	NR	NR	NR	no agency	NR	F	no ops agency	EMSA has no law enforcement missions
agency to agency	Agency EMSA	A111, A21, A311, A331	NR	NR	NR	no agency	NR	F	no ops agency	
information service : to provide a report on ship, ownership and cargo.										
non relevance due to the definition of the service. All public authorities could havec access to the pollution information, but law enforcement is imited										

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

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to MS	MS	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	F	F	F	F	F	F	F	open data, excepted A.1.1.1.9 (IMO number ?) & A.3.2.1.5 Ship owner (could be personal data), but no restriction to exchange between public actors
MS to MS	MS	A.1.2.1 to A.1.2.10	F	F	F	F	F	F	F	excepted limitations to security reasons (Defence). A.1.2.4 must not contain any personal data.
MS TO AGENCIES	MS	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	F	F	F	no agency	F	F	no ops agency	EUROPOL: illicit traficking including cross border crime EMSA: safety and pollution purposes EFCA illegal fishing FRONTEX: irregular migration MAOC-N: drug smuggling EUROJUST: European Arrest Warrant - EAW
AGENCY TO AGENCY	AGENCY (EMSA, EFCA, FRONTEX)	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	F	F	F	no agency	F	F	no ops agency	ditto
AGENCY TO MS	AGENCY (EMSA, EFCA, FRONTEX)	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	F	F	F	F	F	F	F	ditto

A vessel of interest is not a governememtal european vessel

A.1.2 data elements have been removed because they are not open data or they could be sensitive depending on the situation

The request is only the position and route, activity, the customer does not need to have A.1.2 data elements used to confirm the position

In a member state, the provider could be any authorities that possess fixed or mobile sensors.

Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance (Use case 57)

baseline operation

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to Agencies	MS PA	C.1.1	NR	C	NR	no agency	C	NR	no ops agency	Customer Europol and EMSA are not legitimated. EFCA & FRONTEX : limitation of the purpose
MS to MS	MS PA Border control, law enforcement	C.1.1	N	N	N	C	F	F	C	Customs & Defence plan tactical surveillance in some member states
MS to MS	MS PA	C 1.2 & C1.3	C	C	C	C	F	F	F	limitation of the purpose. C1.3 could be anonymous is needed. C.1.2 : could be restricted to open data
MS to MS	MS *Customs*	C.1.1	N	N	N	F	F	F	C	limitation to the defence community in some member states
MS to MS	MS *Defence*	C.1.1	N	N	N	C	C	C	C	limitation of the purpose
MS to MS	MS *Fisheries*	C.1.1	N	C	N	C	F	F	C	limitation of the purpose
Agency to MS	Agency EMSA	C.1.1	F	C	F	C	C	C	C	EMSA chartered vessels (to be assessed) limitation to maritime safety, EUSC ressources could be requested (to be assessed)

to provide information relatives to capacities to a customer, in order to elaborate a plan for basic surveillance in a given sea area

Tactical surveillance planning is coordinated between communities in some member states

The area of responsability of defence communauty is restricted in some member states (no law enforcement responsabilities)

Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance (Use case 57)

targeted operation

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to Agencies	MS PA	C.1.1	F	F	F	no agency	F	NR	no ops agency	for search and rescue purpose
	MS PA	C.1.1	C	C	C	no agency	C	F	no ops agency	Customers : EMSA (safety and pollution communities), EFCA, FRONTEX, EUROPOL case by case basis to reflect the diversity of the possible operations
MS to MS	MS PA	C.1.1	C	C	C	C	C	C	C	case by case basis to reflect the diversity of the possible operations
	MS PA	C 1.2 & C1.3	F	F	F	F	F	F	F	
	MS Defence	C 1.2 & C1.3	C	C	C	C	C	C	C	case by case for some member states
Agency to MS	Agency	C.1.1	F	C	F	C	C	C	C	EMSA chartered vessels (to be assessed) limitation to maritime safety, EUSC ressources could be requested (to be assess)
Agency to agency	Agency	C.1.1	NR	F	NR	no agency	F	NR	no ops agency	EMSA chartered vessels (to be assessed) limitation to maritime safety, EUSC ressources could be requested (to be assess)

to provide information relatives to capacities to a customer, in order to elaborate a targeted operation in a given sea area

information service : detection of vessels cooperating at sea for illegal activities (use case 70)										
example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to Agencies	MS PA	C.2:12; C.6.2.2; C.6.5.5	C	C	NR	no agency	F	F	no ops agency	EUROPOL, probably not direct link. FRONTEX, communication via Eurosur. EMSA, not in the mission of the Agency ! Can receive information when safety is concerned
MS to MS	MS PA	C.2:12; C.6.2.2; C.6.5.5	C	C	NR	F	F	F	F	provider indetermined
	MS Customs	C.2:12; C.6.2.2; C.6.5.5	C	C	NR	F	F	F	F	only direct link between customs
	MS Maritime Safety	C.2.12	F	C	NR	N/F	N/F	N/F	N/F	only direct link between maritime safety. Limitation of the purpose. Shift from N to F need a change in a regulation (VTM directive.)
Agency to Agency	EMSA	A.1.1	NR	NR	NR	no agency	NR	NR	no ops agency	effect of EMSA / FRONTEX agreement ? The group consider the case is not relevant
Agency to Agency	FRONTEX	C.2; C.6.2.2; C.6.5.5	NR	NR	NR	no agency	NR	F	no ops agency	EUROPOL
4 Agency to MS	FRONTEX	C.2; C.6.2.2; C.6.5.5	C	C	NR	C	F	F	F	hypothesis of Frontex own sensors. Frontex regulation limits communication to customs
comments					not concerned				Member states have different views on constitutional of defence tasks	

Information service: Anti-Piracy Maritime Surveillance and free navigation control (use case 85). International waters

example	provider	Data element ref.	Customer (communities)							comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to MS	MS-PA	c.7.3, C.7.6, C.7.7, C.7.8, C.7.10, C.1.1 ?	NR	NR	NR	NR	NR	F	F	operation limited to the recovery of the attacked ship. Some data elements could be considered as EU confidential
MS to MS	MS-PA	C.7.1, C.7:2, C.7.3, C.7.4, C.7.5, C.7.7,	F	F	F	F	F	F	F	global operation including prevention of other attacks
MS to agency	MS-PA	C.7.1, C.7:2, C.7.3, C.7.4, C.7.5, C.7.7,	F	F	F	no agency	F	F	no ops agency	global operation including prevention of other attacks
Agency to MS	Agency: Europol, EMSA, EFCA, FRONTEX	C.7.1, C.7:2, C.7.3, C.7.4, C.7.5, C.7.7,	F	F	F	F	F	F	F	global operation including prevention of other attacks
Agency to agency	Agency	C.7.1, C.7:2, C.7.3, C.7.4, C.7.5, C.7.7,	F	F	F	no agency	F	F	no ops agency	global operation including prevention of other attacks
the service provided is the communication of all data element concerning the case.										
the operation must be undestood as a global operation including preventing attack of other ships, and recovering the attacked ship and its crew										

information service : Detection and behaviour monitoring of IUU listed vessels (use case 93)									
example	provider	Data element ref.	Customer (communities)						comments
			Maritime safety	Fisheries control	Marine Pollution	Customs	Border control	General law enforcement	Defence	
MS to MS	MS Maritime safety	A.1.2, A.2.1, A.2.3, A.3.2.2, A.3.3, A.3.4, C1	NR ?	C	NR	C	C	C	NR	Restricted Access to LRIT etc: Why is there a limitation of access rights for Fisheries ?
MS to MS	MS Fisheries control	A.1.1, A.1.3, A.2.1, A.3, C.6.4, C.2.12	C	C	NR	C	C	C	NR	Restricted access to VMS from other MS: No european vessels in the IUU list
MS to MS	MS Marine Pollution				NR				NR	
MS to MS	MS Customs	A.2, C.2.12, C.6.5	C	C	NR	C	C	C	NR	
MS to MS	MS Border control	A.1.2, A.2.3, A.3.3, C1, C.2.12	C	C	NR	C	C	C	NR	
MS to MS	MS General law enforcement	A.1.2, C.2.12, C.6.5	C	C	NR	C	C	C	NR	
MS to MS	MS Defence	A.1.2, A.3.3, C.2	C	C	NR	C	C	C	NR	
Agency to MS	Agency -EFCA	C.6.4, C.2.12	C	C	NR	C	C	C	NR	Restricted access to VMS from other MS: No european vessels in the IUU list
	Fisheries control-Commission	A.1, C.2.12, C.6.4	C	C	NR	C	C	C	NR	Restricted access to VMS from 3rd country via COM. Doubling with EFCA line ?
MS to Agencies	MS PA	data elements	NR	C	NR	no agency	C	C	NR	
Agency to Agency	Agency EFCA, EMSA, FRONTEX, EUROPOL	data elements	NR	C	NR	no agency	C	C	NR	
the information service is to provide data elements to a customer in charge of a IUU intelligence report										
The IUU vessel list is a public list										

F : Full	
C : on cas by case	
NR : not relevant	

Annex VI – Illustration of information classification

<table>
<tr><th>Pilot projects information categories</th><th>EU classification level</th></tr>
<tr><td>Basic information (data):
Are free to exchange without legal constraints. May be considered as personal data if it permits the identification of a natural person (BMM).
Tracking information originates from sensors, observations etc. which is free to be exchanged inside CISE. Basic information is not open information. The information is produced inside the community using CISE (MARSUNO)</td><td>Not classified</td></tr>
<tr><td>Additional information:
This is information created or enriched mainly through the use of analysis tools. This kind of information is often responding to a specific mission or functionality and will be shared based on user demands inside the CISE community (MARSUNO)
Subject to generic legal conditions for exchange (BMM).
Could be subject to commercial constraints or relative to personal data</td><td>Not classified</td></tr>
<tr><td rowspan="4">Restricted information:
This information is sensitive and cannot be shared freely inside the community using CISE. The main fear is the risk of information leaking that could complicate or endanger an operation (MARSUNO).
Restricted by the law (BMM)
Could be attached to commercial sensitivity
Could include personal data</td><td>EU Restricted
Could be disadvantageous to the essential interests of the EU</td></tr>
<tr><td>EU Confidential
Could harm the essential interests of the EU</td></tr>
<tr><td>EU Secret
Could seriously harm the essential interests of the EU</td></tr>
<tr><td>EU Top secret
Exceptionally grave prejudice to the essential interests of the EU</td></tr>
</table>

Annex VII – Extract from BMM and MARSUNO experiences

A

SHORT PAPER

WP4 - PORTUGAL

| BMM Report – EXTRACT |

The intention for this short paper was to analyze the release of information, using BMM report as a reference, concerning to registers and data bases, ships, national and shared sensors and commercial services. However, the BMM legal premises of analysis were different since this project was mostly focused on data exchange between the member states and, therefore, mainly concerned to registers and data bases.

Indeed, the main aim behind BMM's project that ran in the Mediterranean basin was to test, in the theatre of operations, as to how to effectively integrate maritime surveillance, this in itself being one of the major steps towards the regional integration of the European maritime reporting and surveillance. In other words, BMM went beyond border related aspects, thus covering all maritime activities as it is envisaged by the CISE framework. As for the BMM's legal aim, it was to provide a substantial fieldwork insight into the legal issues and solutions encountered by the parties and the possible solutions. It is important to apply the legal framework, taking due consideration of the legal constraints, yet defining rules that permit the parties to exchange information.

It concluded that a clear legal framework needs to be established, defining at least the nature of the data involved, the capability of the data providers, the purposes (and the methods) of the exchange and the potential recipients of the data. The necessary safeguards with regard to the confidentiality and security of data and the protection of personal data need to be respected by the recipient of the data.

In this specific approach, the main objective of the consolidation achieved in BMM was to underline and reveal the general perspectives and the specifications of each country regarding the most relevant aspects having also into account the significant regimes, systems and mechanisms,

Reporting Regimes

Under this scope are included those regimes whereby data must be actively reported by a person or vessel subject to the applicable regime.

- Data from Automatic Identification System (AIS) can be made available with no restrictions;
- Long-Range Identification and Tracking of Ships (LRIT) data is not shared because contracting states receive the information, but they can´t exchange with another states, it is effectively a closed system. LRIT is not yet fully operational;
- Vessel Monitoring System (VMS) data received is confidential information that is exchanged between the competent authorities of the coastal and the flag state.

Surveillance Systems

Under this scope, BMM included systems under which data is gathered by surveillance methods in respect of which the person who is subject to the scheme plays no active part, as:

- **Vessel Traffic Services (VTS)**: There are two basic types of VTS – coastal and port. In terms of international law the legal regime for VTS is contained in Regulation 12 of SOLAS supplemented by guidelines adopted pursuant to IMO resolution A. 857(20) of 27 November 1997. At EC level, VTS is addressed in Articles 8 and 9(3) of the VTM Directive.

  The information received from VTS is made available of on a selective and secure basis;
- **Military Surveillance Systems**: The gathering of surveillance data is inherent to the role of Europe's navies for defense purposes, which since 2001, includes defence against terrorism;
- **Cleanseanet**: CleanSeaNet is a satellite-based monitoring system for marine oil spill detection and surveillance in European waters provided by the European Maritime Safety

Agency (EMSA). EMSA obtains radar satellite images from commercial satellite providers according to action planned with MS.

- **Sistema Integrado de Vigilancia Exterior (SIVE)** : Operated by the Spanish Guardia Civil is a Coastal surveillance system that is based on a network of fixed stations and mobile units that make use of still cameras, CCTV, radar and infra-red sensors.
- **SIVIIC** – Operated by the Portuguese National Republican Guard, is an Integrated Surveillance System.

Data Sharing Mechanisms

These are different mechanisms currently exist for sharing maritime surveillance data, concerning to a range of different purposes and stockholders. They provide for the sharing of maritime surveillance data both internationally and within individual Member States, as:

- **SPATIONAV** – National data sharing mechanism: designed to collect and compile data generated by a range of sensors to assist maritime operational centres.
  France information managed by the navy which is connected to Trafic 2000 and SafeSeaNet.
- **Regional AIS**: The HELCOM AIS Network enables the real time sharing of AIS data among the parties to 1992 Helsinki Convention ;
- **SafeSeaNet**: is a data exchange system developed by EMSA to support the implementation of elements of the VTM Directive ;
- **Commercial AIS**: AIS Live is owned by Lloyds Register Fairplay Limited and the acess to the service is by subscription ;
- **Virtual Maritime Traffic Centre (V-RMTC)**: Virtual network connecting the operational centres of number of navies that enables the sharing via internet of unclassified information on merchant shipping; Coordinated by the Italian Navy.

Concerning **data**, different categories of information were identified regarding basic data, additional data and restricted data, meaning that:

- **Basic data** are exchangeable with no legal constraints, although it's important to be aware that, for instance, information regarding ship owner and ship company, as well as ship photograph, may be considered personal data if permit the identification of a natural person.

- **Additional data** are accessible from certain selected sources although it's subject to generic legal conditions for exchange (e.g. purpose related, or subject to third party licensing, etc). Usually referenced as case by case analysis;
- **Restricted data**, which availability is restricted by law.

The information to be exchanged is categorized from the access restrictions based on the BMM Matrix, as described:

Green: Data available for sharing in the whole BMM community.

Blue: Data available for sharing in limited sectorial communities.

Orange: Data available for sharing with respect to legal restrictions.

BASIC DATA

Positional Data

Track number or label
Position latitude and longitude
Time GMT
Course
Speed
Navigational status
Type of sensor
data provider

Current Voyage Data

Port of origin
Last port of Call
Time of Departure (ETD + ATD)
Port of destination
Estimated Time of arrival (ETA +ATA)
RoutePlan

Cargo(IMO class+ quantity)
Cargo (other than IMO class)
Draught
Total number of persons on board
ISPS level
Platform limitations

Basic ID Data

Name
Yearofconstruction
Type
Hull main color
Numberofmasts
propulsiontype
Shipmaximumspeed
Length
Beam
Max draught
Grosstonage
Deadweight
Port of registry
Flag
Ship owner*
Ship company*
IMO number
MMSI number
International RadioCall Sign
Classification society
Ship photograph*

GMDSS class
Activity

* REMINDER - Information regarding ship owner and ship company, as well as ship photograph, is to be considered as "personal data" if it relates to the identification of a "natural person".

Other Data

Satellite Imagery*
Environmental information (detail what info) (SERV)
METOC data (SERV)
Insurrance coy
Ship agent
Environmental INCIDENT (BASIC DATA)
Safety INCIDENT REPORT (UNCLAS)(BASIC DATA)

* **REMINDER** - Information regarding satellite imagery is to be considered as "personal data" if it relates to the identification of a "natural person".

ADDITIONAL DATA

Current Voyage Data

Events related with last port
Master/Captain details
Crew list
List of persons o/b
Elements of suspicion of the persons on board
Latest report

Historical Data

Ship name history
Ship ports history
Ship flag history
Ship ownership history
Ship routes history
Ship MMSI history
Port State control history
Elements of suspicion of the vessel

Other Data

Intelligence
ALERTS*
Infrastructure*
Elaborated Sectorial Information

*__REMINDER__: classified according to the classification of the original information/data and the classification agreed upon by the users actors.

Within the scope of specific potential **legal restrictions**, the purpose behind the sharing of data shall be a fundamental pre-requisite to any data sharing mechanism. A clear and precise description of the purposes behind the data exchange mechanism is therefore of crucial importance (e.g. illegal trafficking and immigration) in the same manner as the respect of the legality and proportionality principles.

The main legal instruments to have in account are the Council Framework Decision 2006/960/JAI of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the member states of the European Union and the Convention on Mutual Assistance and Cooperation between customs administrations (Naples II).

The main texts at the European level concerning **personal data** protection are:

- Directive 95/46 of the European Parliament and the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personnal data and the free movement of such data
- Council Framework Decision 208/977/JHA of 27 November 2008 on the protection of personnal data processed in the framework of police and judicial cooperation in criminal matters
- Laws relating to data protection at the national level should also be taking into account.

WARNING – Information regarding the ship agent, as well as ship photograph, is to be considered as "personal data" if it relates to the identification of a "natural person".

Personal data is not to be processed for purposes other than those for which they were collected.

Specifically in relation to the sharing of personal data, purpose-limitation and proportionality are fundamental principles which need to be taken into account.

Processing of personal data is an "identified" potential restriction on data sharing the name of a vessel is not sufficient to directly identify a (natural) person owning a vessel.

However, the unique combination of the vessel name with other data elements, such as a unique vessel registration number, that enable the identification of a single person (vessel owner, captain, crew, etc) may amount to personal data. Furthermore, pictures, including CCTV images and other visual data may also be considered personal data if they permit the identification of a natural person.

Taking the above into account, analyzing maritime surveillance data we can conclude that some data involve personal data (e.g. where data concerns a fishing vessel identification number, a license number or external registration number or other unique identifiers that can lead directly or indirectly to the identification of a natural person). While in the majority of cases the owner or agent of a vessel will be a legal person this may not always necessarily be the case.

Regarding **confidentiality**, it can be originated through legislation due to the inclusion of express legal provisions to this effect.

While certain legal provisions are not to debar, as such the exchange of data, recipients of such data are duty bound not to disclose it to third parties not specifically mentioned within the relevant legal framework (with regard to confidentiality provisions imposed by contract one example is the standard agreement of Lloyds register Fairplay Limited relating to AIS Live which imposes the "duty of confidentiality" on users and effectively prohibits unauthorized third party re-use). Similar provisions emanate from the end user licence for CleanSeaNet, including a purpose limitation, the effect of which is the MS may use the data solely for the purpose of oil spill monitoring.

Also, a significant amount of surveillance data is qualified and/or has to be treated as **(commercially) confidential**. As a consequence, the processing of this data will be affected by the duty of confidentiality and professional secrecy of the persons authorized to have access to the data.

WARNING - Sometimes there is contractual confidentiality that doesn't permit the information sharing (v.g. Lloyds Data Base).

With regard to the use (including the sharing) of maritime data, sectorial legal provisions may impose specific restrictions (such as limitations on the purpose of the use or on the type of actors that may have access to the data). Additionally, it should be taken into account that, if the sourcing of sharing of data is taking place on a contractual basis (for instance, where data are acquired from commercial suppliers), such contracts may also contain specific restrictions (for instance, contractual provisions on intellectual property rights may limit the user's right to reproduce, exploit and share the data).

B

MARSUNO paragraph 4.4 (Legal obstacles) Summary

“The key approach for achieving a functional, efficient and performing CISE is to create a stable, foreseeable and accessible basis for exchange of information. The essential wording is ‘harmonization of legal conditions’.

Respect for the fundamental rights of people includes rights of privacy and consequently also protection of personal data. The right to process such information is well-balanced to serve society’s needs for information in order to ensure its development at all levels and for the protection of peace, liberty and democracy. Any further enlargement of the possibilities to transfer personal data has to ensure the protection of this fundamental right. The majority of data/information relevant to the needs within the maritime community, regardless of whether it is personal or non-personal, is, from a legal point of view, already fully accessible at any moment for the stakeholders involved. Most reasons for accessibility constraints are due to administrative procedures and technical barriers. Nonetheless, some obstacles of a legal nature have been identified. Some are of such nature that a solution would need a material adaptation of the running legislation, i.e. positive change of the rule itself, e.g. change from a prohibition to a (complete or partial) permission. Some obstacles could be removed by a simple structural change of the legislation in place. Some problems are not purely legal as such, but result from a policy approach. Changing the policy approach would consequently also change the grounds for the legal framework and its content.

The prevailing conclusion on the concept of information exchange problem is due to incompatibility because of the disparity of national legislation given within the margins of maneuver provided for by the applicable European legislation. A conclusive approach for a solution may then focus on harmonizing legislation, either directly detailing the provisions on European legislation level or directing further the implementing margins.

In addition, as changes of legislation on the EU level are time consuming procedures, and at the same time the need for the right information at the right time is noted, the only viable solution at hand is to get all stakeholders to act in the rather simple and efficient procedure of entering into agreements with each other while the more formalistic and political alternatives are proceeding.

Lastly, to ensure the necessary adaptations over time and implementation of the results on a broad scale as simultaneously as possible to satisfy the needs for relevant information within the user communities involved it will be required that the alterations are well founded throughout the communities, inside and outside the Union. Such conditions call for political involvement, while the development procedures should be carried out in close cooperation by the stakeholders. This demands a program-like procedure, which could be harnessed by a policy, monitored and lead by the European Commission.”

Annex VIII – Output classification with regards to personal data

Use case	Output data element	TAG data matrix reference	Include personal data
13b	Intelligence report	A.2.2, C.6.2, C.6.5	May be
13c	Intelligence report	A.1.1, A.2.3, A.3.2, C.6.3, C.8.2	Yes
25	Intelligence report	A.1.1.1, A.2.1, A.3.1.1, A.3.3.1	May be
44	Vessel data report	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	A.3.2.1.5 may be personal data
57	Ressources information	C.1.1, C.1.2, C.1.3	No
70	Intelligence report	C.2; C.6.2.2; C.6.5.5	No
85	Piracy Information	C.7	No
93	IUU vessel information	A.1, A.2, A.3, C.2.12, C.6.4, C.6.5	May be

Annex IX – Purposes versus Use Cases

Sector	Purpose	Use Case							
		13b	13c	25	44	57	70	85	93
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								

Annex X – Reminder for studies of access rights within the Use Cases

This reminder explains how the access rights issues of the different use cases could be studied in order to elaborate the access rights matrixes.

The lines of the matrix describe different examples to study the different situations. There are at least four cases:

provider	**customer**
Member state public actor	Member state public actor
Member state public actor	UE agency
UE agency	Member state public actor
UE agency	UE agency

Inside one member state, it is desirable to identify the user community. It is important to know that, depending on the organization of the member state, the community can include several public actors.

The study must be carried out to get answers to the following questions:

What is the TAG data matrix reference of the data elements in output of the information service?

Is the provider self-sufficient in providing the service? If not, is it legitimated?

Is the customer legitimated to receive the information? Is it in its missions? What is the link with the ship concerned with the information (state of owner, state of flag, port of departure, port of destination, state of transit,)?

Is there a legal text that imposes upon the information exchange?

Is there a legal text allowing the exchange?

Is there a legal text prohibiting the exchange?

Is the pattern consistent with legal text and sensitivity issues?

What legal basis change would be useful?

Example: the “Swedish decision” 2006-960, imposes upon an answer to a State, it allows the exchange between law enforcement authorities, but it does not impose upon a broadcast communication.

How could the exchange be done today (room for CISE technical improvement)?

The matrix must be filled using only three letters:

- F: for full access
- C: for case by case access,
- N: for ”no access at all”, or NR for ”not relevant”.

“F” and “C” could be desirable access, not possible today. In that case, the matrix can be filled with two letters as:

“C / F “, where the first letter corresponds to the present situation and the second corresponds to the desired situation.

“N” no access must be justified with sensitivity issues.

The column “comments” must be used to summarize the main issues of the example.

Annex XI – Coverage of TAG data matrix

TAG Data elements	Use cases								comments
	13 b	13c	25	44	57	70	85	93	
A.1.1		X	X	X					
A.1.2								X	
A.1.3									Not used
A.2.1		X	X	X				X	
A.2.2	X								
A.2.3		X						X	
A.2.4									Not used
A.3.1		X	X	X					
A.3.2		X		X				X	
A.3.3		X	X	X				X	
A.3.4		X						X	
A.4									Not used
A.5									Not used
B.1									Not used
B.2									Not used
C.1					X			X	
C.2						X		X	
C.3									Not used
C.4									Not used
C.5									Not used
C.6	X	X				X		X	
C.7							X		
C.8		X							
C.9									Not used
C.10									Not used
C.11									Not used

Annex XII – Classification of information services / EU classification levels

Use case	Output data element	Not classified	EU restricted	EU confidential
13b	A.2.2, C.6.2, C.6.5		X	
13c	A.1.1, A.2.3, A.3.2, C.6.3, C.8.2	X	X	
25	A.1.1.1, A.2.1, A.3.1.1, A.3.3.1	X		
44	A.1.1, A.2.1, A.3.1, A.3.2, A.3.3	X		
57	C.1.1, C.1.2, C.1.3		X	
70	C.2; C.6.2.2; C.6.5.5		X	
85	C.7		X	X
93	A.1, A.2, A.3, C.2.12, C.6.4, C.6.5	X	X	

Annex XIII – List of possible observed deficiencies of access rights and lack of needed information

- Information services must be developed with legitimated providers and customers. The pattern must be assessed properly. Input data has to be considered (as other services).
- Exchanged with third parties must be studied.
- Personal data must be excluded of the data elements as much as possible (ship photograph, contact information, IMO number, …)
- Lack of surveillance sensors in high seas.
- Some data elements of the TAG data matrix are not explicit (“activity”).
- There is no information about the consideration of the needs for CISE in the revision of Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system.
- There is no information on the possible existing flow of information using current way of communication (EMSA informations systems, EUROSU, MARSUR, SIENA …).
- Lack of information on classification system used by the public authorities.
- Lack of information systems and network able to handle EU restricted information. No IT network to exchange EU confidential information.
- Lack of knowledge of procedure used by other authorities to handle personal data.
- Interpretation possible on the fact that some data elements are or are not “personal data”: creates legal uncertainty.
- Limitation of communication exchanges in the Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system (purpose safety).