DIGIT – DIRECTORATE GENERAL INFORMATICS

DG MARE – DIRECTORATE GENERAL MARITIME AFFAIRS AND FISHERIES

JRC – JOINT RESEARCH CENTRE

CISE Architecture Visions Document

[Study supporting the Impact Assessment]

Date: 06/11/2013
Version: 3.00

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Office: 05/45. Telephone: direct line (32-2) 2999659.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

Document Control Information

Settings	Value
Document Title:	CISE Architecture Visions Document
Project Name:	Common Information Sharing Environment (CISE)
Document Authors:	DIGIT / DG MARE / JRC
Project Managers:	Marta Silva Mendes (DIGIT); Olivier Fontaine (DG MARE)
Revision Status:	3.00
Issue Date:	06/11/2013

Document Approver(s):

(All Approvers are required. Records of each approver must be maintained.)

Approver Name	Role
Beate Gminder	Head of Unit; D1 DG MARE

Document Reviewers: (Records of each required reviewer must be maintained.)

Reviewer Name	Role
Isabella Perret	Team Member; DG MARE
Isto Mattila	Team Member; DG MARE
Marta Silva Mendes	Project Member; DIGIT
Olivier Fontaine	Project Manager; DG MARE
Staffan Ekwall	Team Member; DG MARE
Thomas Strasser	Team Member; DG MARE
Alessandra Zampieri	Head of Unit; JRC
Franco Oliveri	Team Member; JRC
David Berger	Team Member; JRC

Summary of Changes:

The Document Author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, spelling and clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarised in the following table in reverse chronological order.

Revision	Date	Created by	Short Description of Changes
V2.04	04/10/2013	DIGIT/DG MARE	Adapted to take stock of the results of the Impact Assessment and the Gartner Study.
V2.51	07/10/2013	DIGIT/DG MARE	Update of definitions and executive summary.
V2.52	07/10/2013	DIGIT/DG MARE	Update “Key Concepts” and remove mentions of a White Paper

V2.55	10/10/2013	DIGIT/DG MARE	Update the impact assessment summary image and the addition of clarifications
V2.56	25/10/2013	DIGIT/DG MARE	Replace section 6.3 with previous version and remove Annex 5 related to the System Impact Analysis
V2.57	05/11/2013	DIGIT/DG MARE	Minor corrections following a check by DG MARE and complete layout, spelling, grammar and page numbering check
V 3.00	06/11/2013	DIGIT/DG MARE	Minor layout corrections (white pages and picture quality)

Configuration Management: Document Location

The latest version of this controlled document is stored in:
https://webgate.ec.europa.eu/CITnet/confluence/display/CISE/D2+-+CISE+Architecture+Vision+Document

EXECUTIVE SUMMARY

The current set up of maritime surveillance activities in the EU leads to a partial understanding of occurrences at sea. According to Regulation (EU) No 1255/2011 establishing a Programme to support the further development of an Integrated Maritime Policy:

"The primary objective of the Union's Integrated Maritime Policy ('IMP') is to develop and implement integrated, coordinated coherent, transparent and sustainable decision-making in relation to the oceans, seas, coastal, insular and outermost regions and in the maritime sectors." [1]

Presently, seven maritime surveillance functions collect data separately and often do not share the data. These functions – (1) maritime safety (including search and rescue), maritime security and prevention of pollution caused by ships, (2) fisheries control, (3) marine pollution preparedness and response, (4) customs, (5) border control, (6) general law enforcement and (7) defence – are here forth referred to in this document as User Communities or sectors. [2] The current fragmentation of information is the result of a large collection of initiatives and information sources in the seven User Communities, both at the EU and national levels. To break across these information silos, considerable effort has been made in recent years to better integrate maritime surveillance information across sectors and Member States according to CISE's roadmap [6]. A main value of integrating maritime surveillance information surveillance is to enhance the present maritime awareness pictures of the sectorial User Communities.

In 2009, the European Commission put forward a communication towards a 'Common Information Sharing Environment (CISE) for the surveillance of the EU maritime domain' and, in 2010, adopted a six step roadmap to achieve it. Under the leadership of DG Mare, the Commission set up a Technical Advisory Group ('TAG') and a Member States Expert sub-Group ('MSEsG') to advise on all steps moving forward. It further involved Member States in the MARSUNO and BlueMassMed pilot projects to verify the value of CISE in practice, and to explore ways to overcome existing barriers to its realisation. In parallel, the Council supported the European Commission in various conclusions [10] and asked for CISE to be operational by 2020.

With the aim of increasing the efficiency and effectiveness of maritime surveillance, CISE should address the current legal, technical and cultural barriers in the sharing of maritime data to allow the sharing of available information across the seven aforementioned User Communities throughout the EU/EEA. A key component of a CISE vision is to facilitate automated exchanges of structured information going beyond simple collaborative tools such as audio and video conferencing, e-mail, etc. In this context, information sharing is to be organised in a decentralised manner, and is to build upon existing and planned User Community systems, which have developed at different speeds and have reached different levels of maturity. To do so, current barriers to interoperability need to be removed through appropriate interoperability agreements at legal, organisational, semantic and technical level, as defined by the European Interoperability Framework (EIF) [3]. Therefore and for the purpose of this document, CISE is described as a collection of Architectural Building Blocks defined in a set of interoperability agreements that enable CISE participants to share information through interoperable digital services.

Building upon the above requirements, the existing and planned systems, the results of the MARSUNO [4] and BlueMassMed [5] pilot projects, as well as other studies, the present document provides:

i.) a catalogue of CISE related principles (Chapter 4) and requirements (Chapter 5);

ii.) the corresponding CISE Core building blocks (Chapter 2 and Chapter 3); and

iii.) the CISE Core vision with three possible architectural visions and a so-called hybrid vision, which reflect upon possible ways of organising CISE throughout the EU (Chapter 6).

The catalogue of CISE related requirements included in this document provides detailed information about the different types of needs that have so far been identified, and does not impose any technological constraints. Please note that this document is not technical in nature, and only touches upon the visions' Architectural Building Blocks, not the Solution Building Blocks. Once the preferred vision for CISE is identified, the actual Solution Building Blocks are to be selected while taking into account the need to minimise the impact on operational information systems and to protect planned investments. As the reuse of existing specifications, services and systems is a priority, it is important to note that these Solution Building Blocks do not need to be built from scratch.

The table below introduces the architecture visions highlighting some of their unique aspects.

ID	Architecture Visions names
Core	**Multiple Providers of CISE Services at National level (+ EU initiatives)** The CISE Core is not a vision like the others. The purpose of the CISE Core to describe CISE's minimum viable architecture as a basis for defining the other visions. Therefore, it does not prescribe a governance model. As the minimum required architecture, the building blocks of the CISE Core Vision are also represented in all other Visions.
A	**Multiple Providers of CISE Services Coordinated by User Communities (+ EU initiatives)** This vision proposes a governance model centred on User Communities. Ideally each User Community should have a single service provider at national level and one or more EU led initiatives. Consequently, the integrated maritime awareness pictures available in CISE are divided by User Community.
B	**Multiple Providers of CISE Services Coordinated by Member States (+ EU initiatives)** This vision proposes a governance model where each Member State appoints an authority to manage which CISE services are delivered by one or multiple service providers. CISE services are also be provided by EU led initiatives. As in Vision A, several integrated maritime awareness pictures coexist, but they are no longer divided in User Communities.
C	**Single National Providers of CISE Services (+ EU initiatives)** This vision proposes a governance model where each Member State appoints an authority to manage which CISE services are delivered. Unlike vision B, each Member State has a single service provider of CISE services. CISE services can also be provided by EU led initiatives. Unlike visions A and B, a single integrated maritime awareness picture can be offered per Member State. Sea basin authorities can also be set up to provide sea basin level services (variant of vision C).
Hybrid	**A merge of Visions A, B and C (+ EU initiatives)** The hybrid vision is created by merging the interoperability agreements of Visions A, B and C. The hybrid vision will make it possible for Member States to decide whether to nominate a single or multiple providers of CISE services at national level. This means that a provider of CISE services at national level may be nominated to deliver CISE services of interest for one or more User Communities. The delivery of CISE services may be done through the improvement of existing and planned systems (such as the National Single Window or National Coordination Centres). Depending on the choice made by the Member State, a single integrated maritime awareness picture exists or several integrated maritime awareness pictures coexist.

The CISE architectural visions capture and compare different views of stakeholders. For example, while some stakeholders asked for a User Community centric approach (vision A), some may prefer the architecture used in the BlueMassMed pilot project (vision C). Meanwhile, others may prefer to introduce some modifications

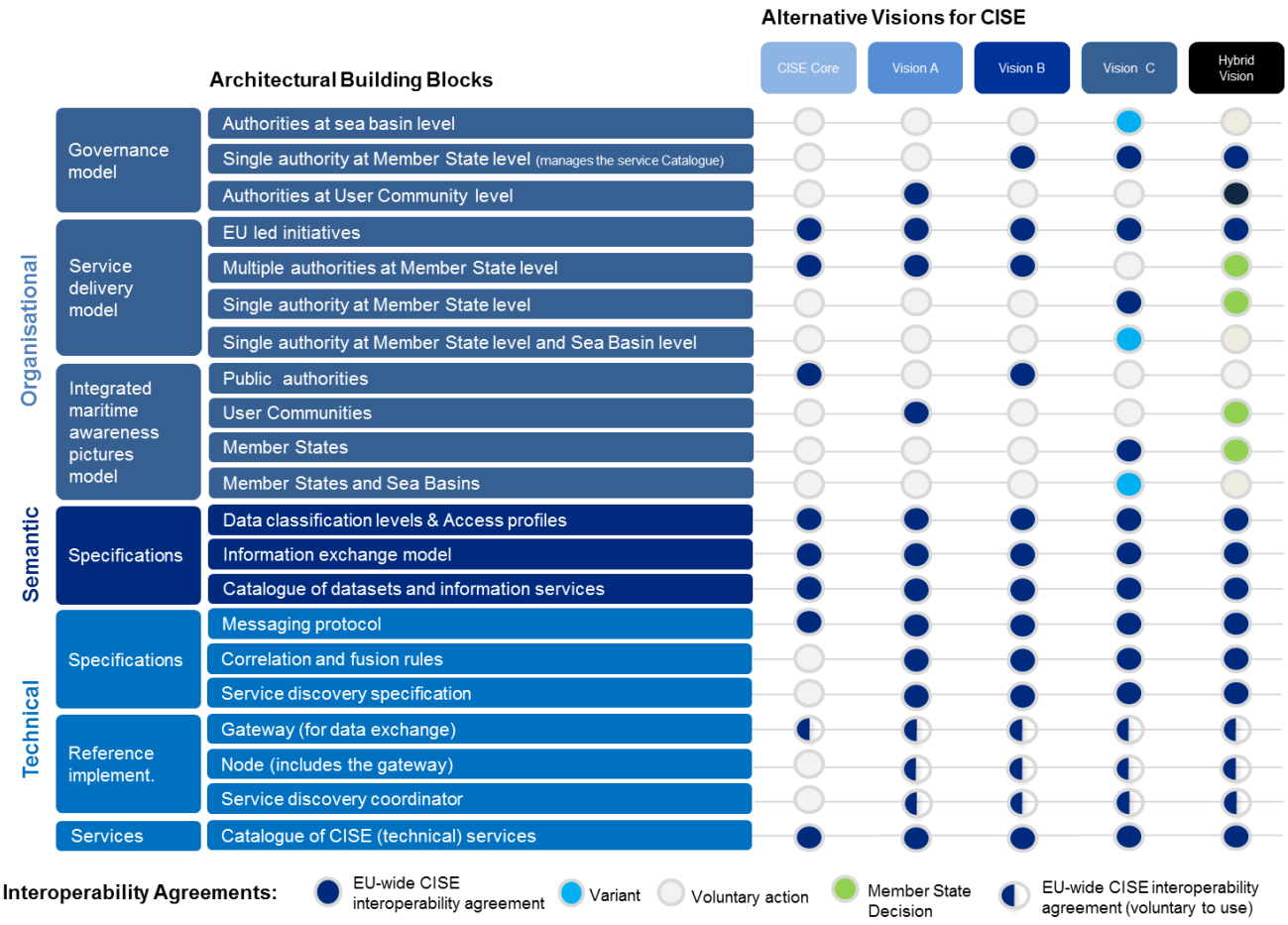
to the latter (vision B). The hybrid vision mixes these preferences depending on the choice made by the Member State.

The main purpose of each architecture vision is to identify ways to eliminate existing barriers to interoperability. Thus, once a preferred CISE vision is identified, these barriers may be removed accordingly, at which point the selected vision's building blocks become interoperability agreements. These visions are meant to explain how it will be possible to interlink the approximately 400 public authorities[1] in the seven User Communities throughout Europe. This document applies a high-level approach based on Architecture Building blocks, not Solution Building Blocks. In existing or planned systems similar Building Blocks are already present, normally established by law. Therefore further consideration of the Solution Building Blocks will be needed at a later stage. It is important to consider both viewpoints, first, looking into unexploited opportunities through the selection of CISE's Architectural Building Blocks, and second, building upon existing systems which allows exploiting what already exists with a view to avoid duplication.

As explained in CISE's roadmap [2], the value of integrating maritime surveillance is to enhance the present sectorial maritime awareness pictures with additional information. CISE will make this possible by promoting the set-up of information services according to common specifications. A CISE information service aims to make available to CISE participants, raw, consolidated or fused data in one or several geographical areas and/or maritime functions. Raw data is considered basic information collected from a source and which has not been subjected to processing or any other manipulation. Consolidated and fused data is considered the collection and integration of data from multiple sources regarding the same data object.

The figure below provides a summary of the Architectural Building Blocks and interoperability agreements present in each vision.

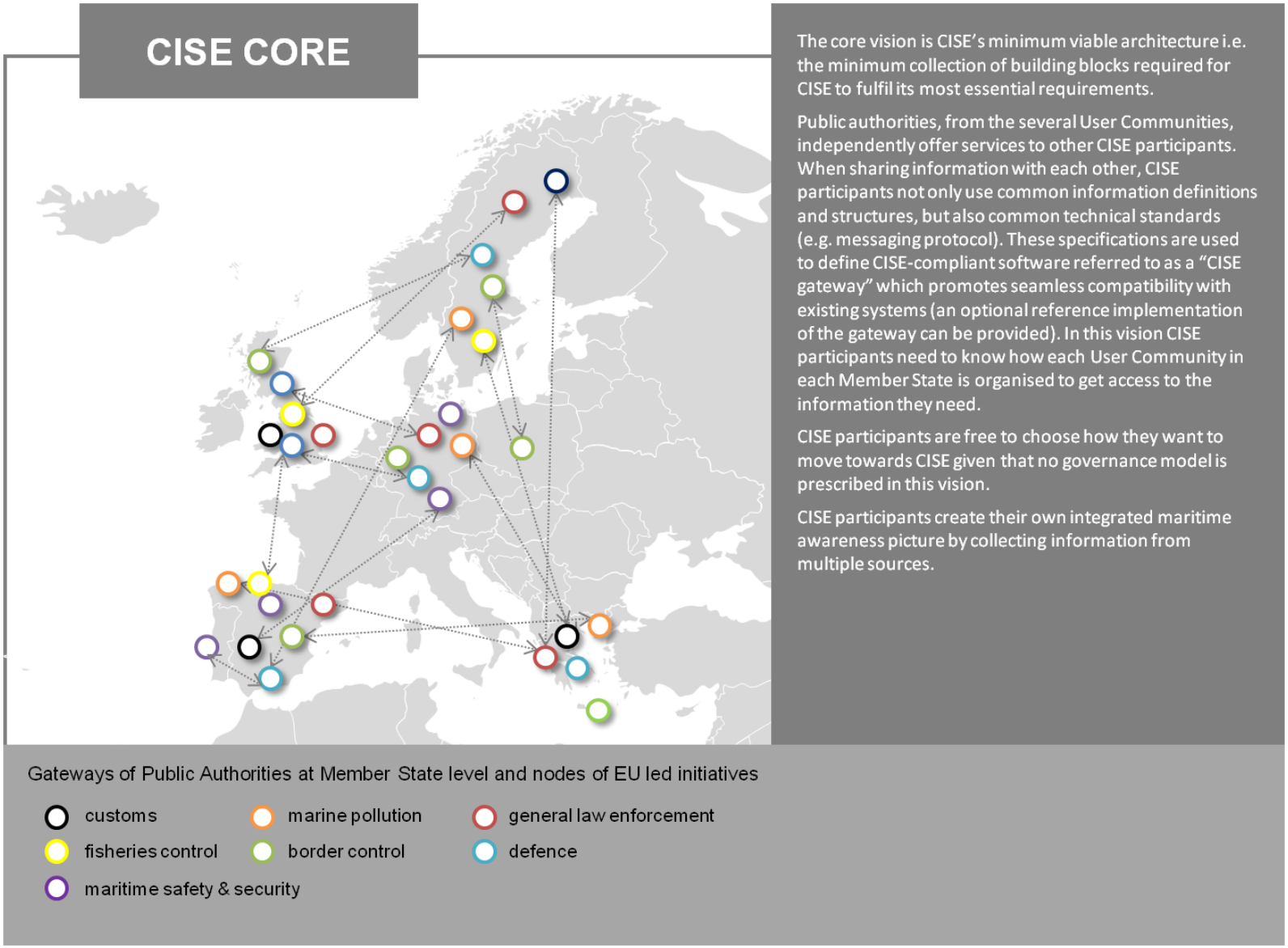
[1] The number of public authorities to be interconnected depends on the governance model and vision chosen for CISEI. Independently of this choice, all 400 public authorities will be interconnected, either directly or indirectly.



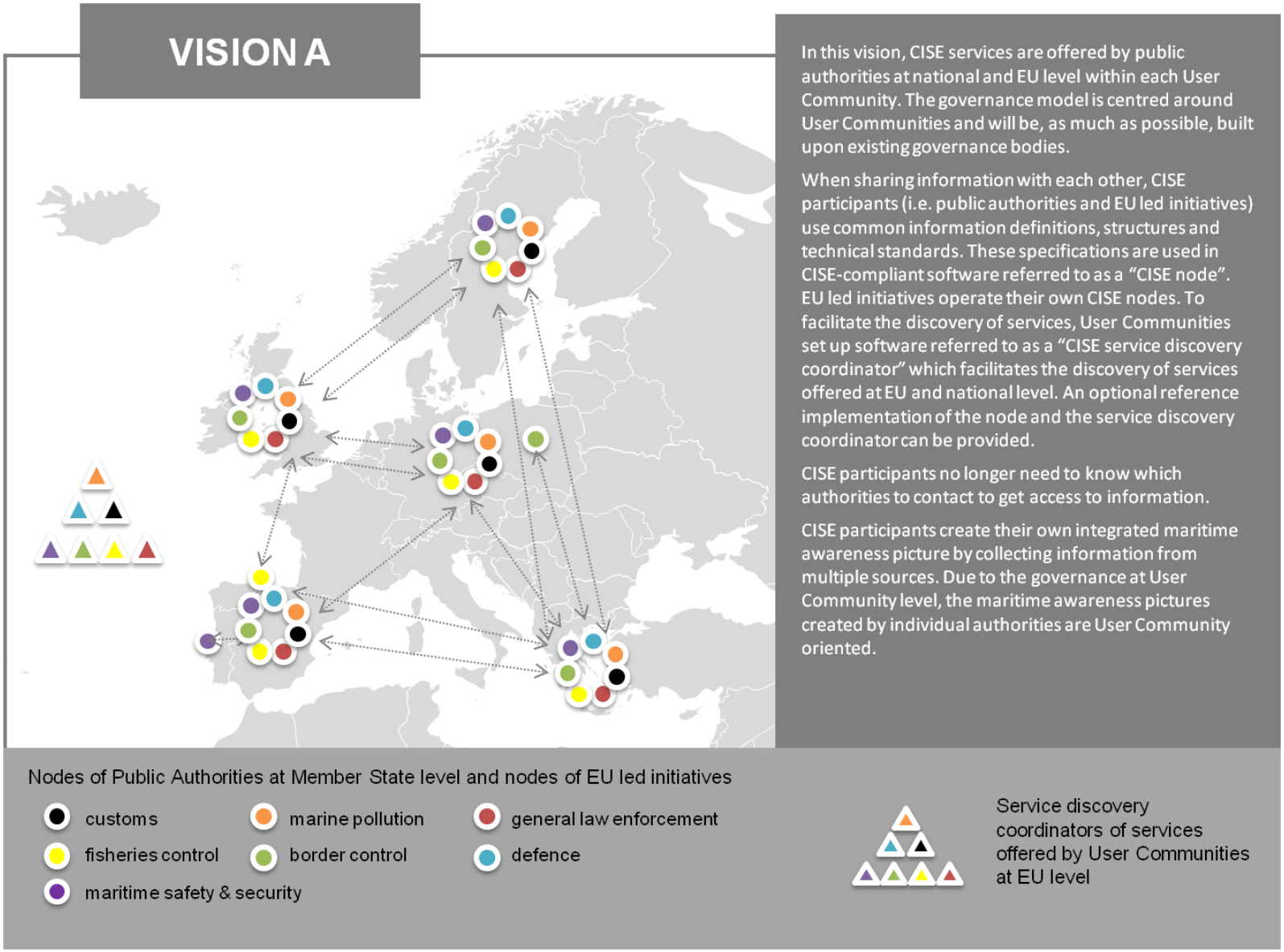
In addition to the above set of interoperability agreements, a supplementary set of real-time collaboration tools should be provided to allow CISE participants to easily interact with one another.

The visions are introduced below as one-page descriptions. It should be noted that the figures are a simplification and therefore do not show every detail about every Member State and every EU led initiative.

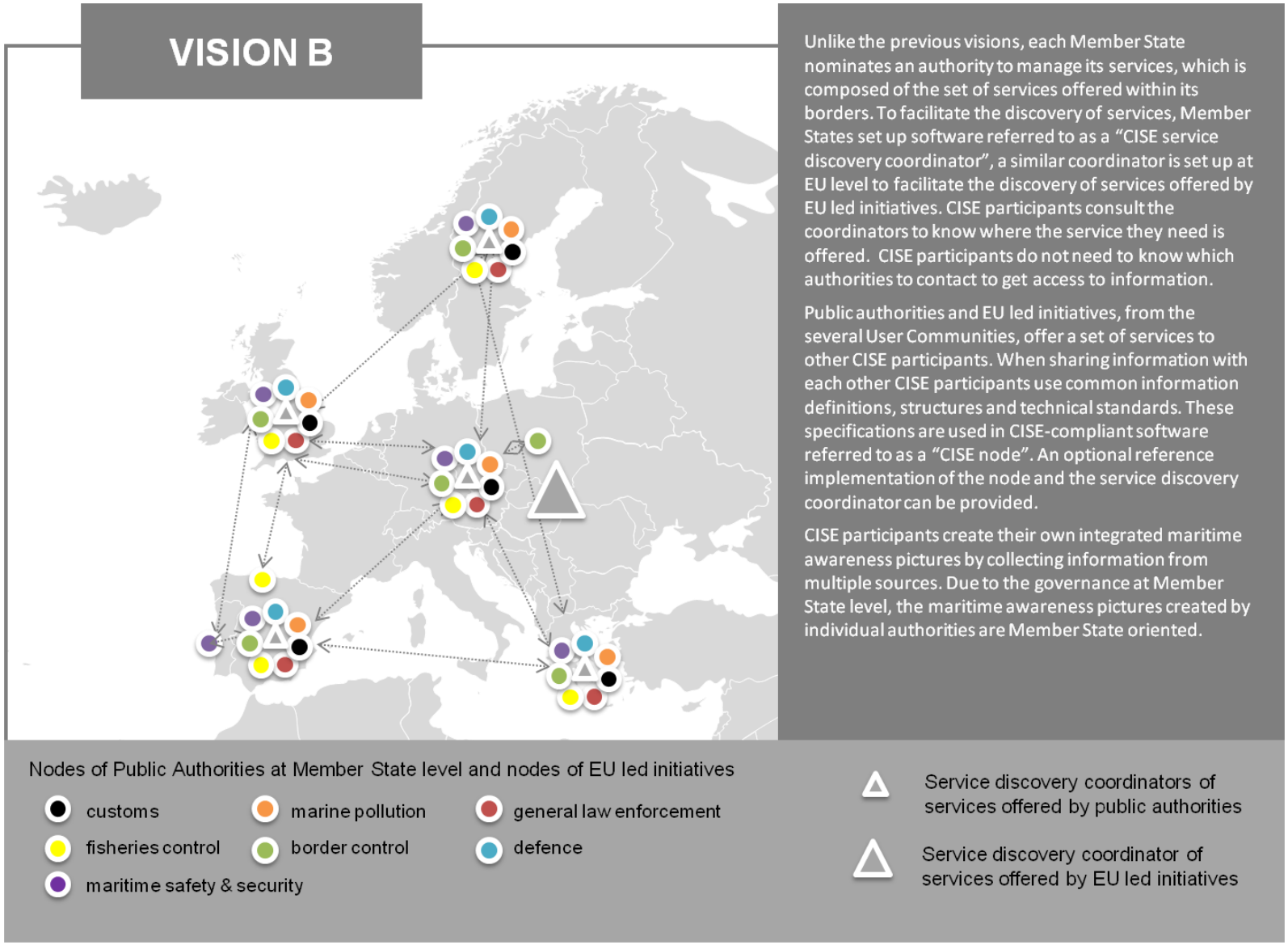
CISE CORE: Multiple Providers of CISE Services at National level (+ EU initiatives)



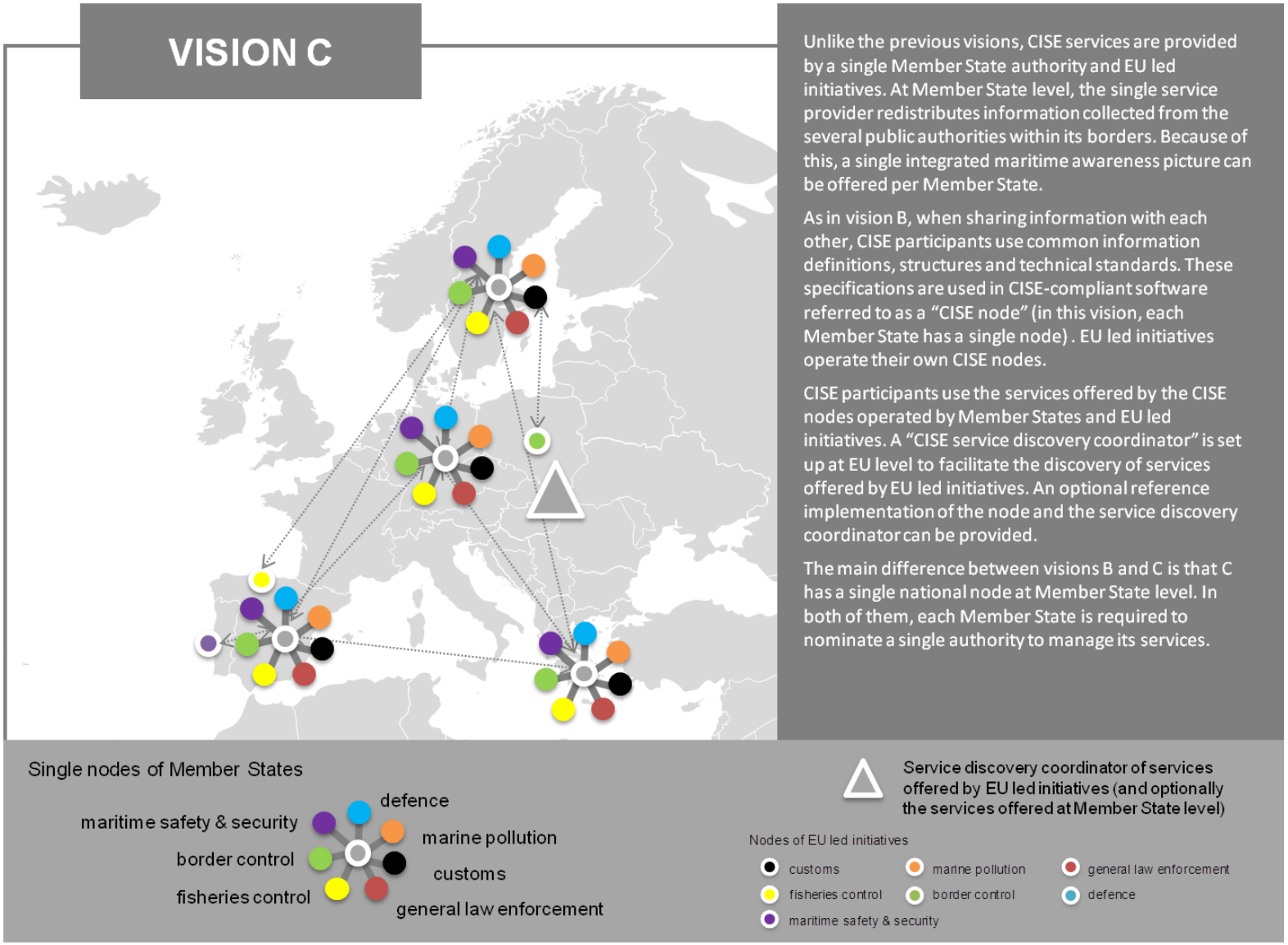
Vision A: Multiple Providers of CISE Services Coordinated by User Communities (+ EU initiatives)



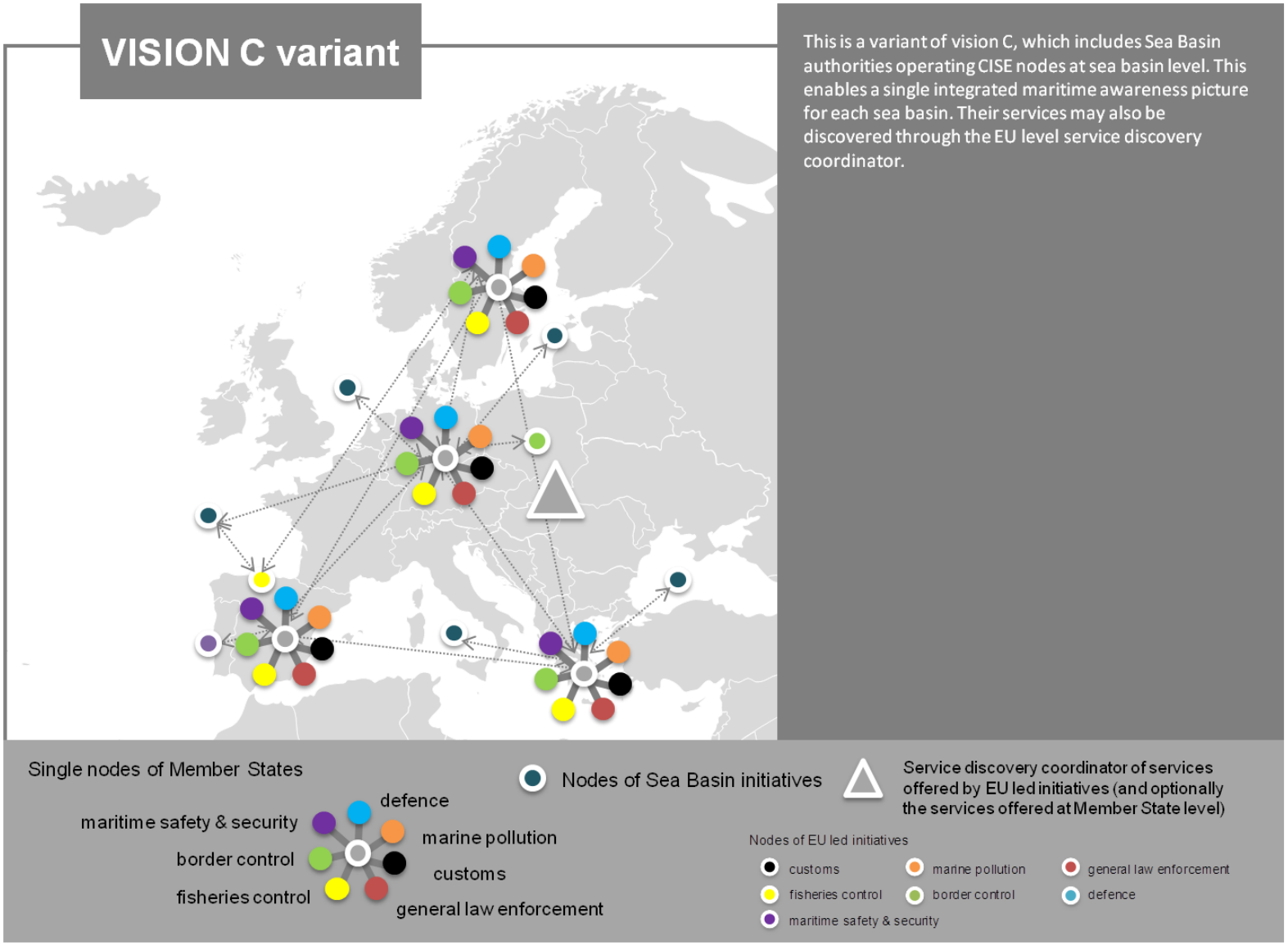
Vision B: Multiple Providers of CISE Services Coordinated by Member States (+ EU initiatives)



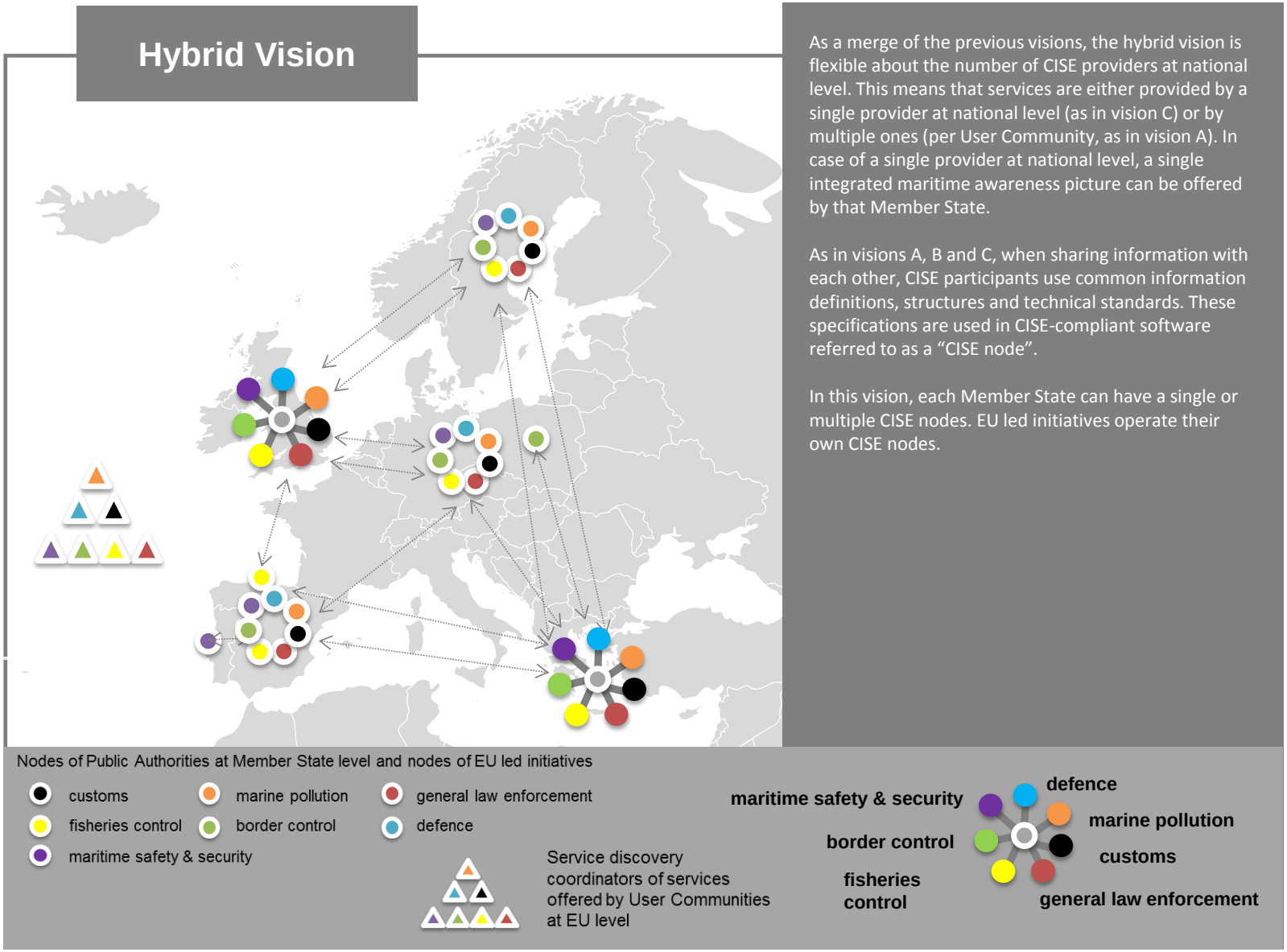
Vision C: Single National Providers of CISE Services (+ EU initiatives)



Variant of Vision C: Single National Providers of CISE Services (+ Sea Basins and EU initiatives)



Hybrid Vision: A merge of architecture visions A, B and C



The following figure shows the requirements' coverage, cost efficiency and IT sustainability of every vision.

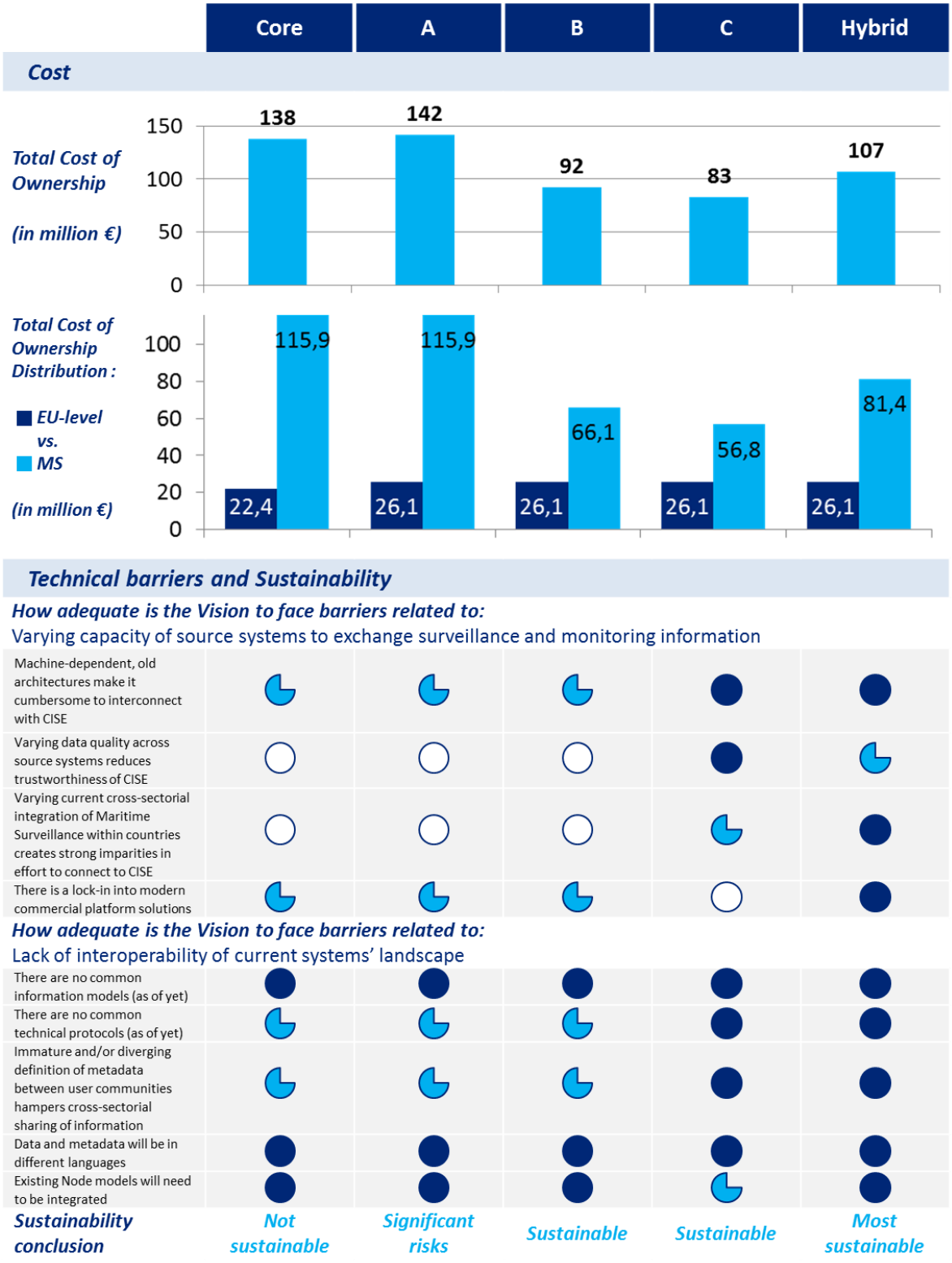


Figure 1 - Requirements coverage, cost efficiency and IT sustainability of every vision. [2]

[2] Source: Sustainability and Efficiency of Visions for CISE, Gartner, September 2013

The data above confirms that Vision C is the least costly and covers the highest percentage of identified requirements. It is also the only vision that addresses the issues of varying data quality of different information sources. The strengths of Vision C come with the trade-off. Vision C imposes the obligation to Member States of setting up a single national Node. As flexibility is very valued by Member States, the Hybrid Vision was created following a request by the Member States' Expert sub-Group on the Integration of Maritime Surveillance after the first release of this document. The Hybrid Vision enables Member States to choose whether to organise themselves around User Communities (as in Vision A) or around the single national Node model (as in Vision C). At the same time, the Hybrid Vision leaves room to Member States to keep their national definition of a User Community (similar to Vision B). Though the Hybrid Vision leaves much flexibility to the Member States, a catalogue of services will have to be created and managed by every Member State.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1. Context

Maritime surveillance refers to the effective understanding of all activities carried out at sea that could impact the security, safety, economy or environment of the European Union and its Member States[3]. Seven different functions, also referred to as User Communities or sectors, were identified as relevant for maritime surveillance: (1) maritime safety (including search and rescue), maritime security and prevention of pollution caused by ships, (2) fisheries control, (3) marine pollution preparedness and response, (4) customs, (5) border control, (6) general law enforcement and (7) defence. The way maritime surveillance is currently set up in the EU does not enable information sharing to the desired level across the seven User Communities, and leads to inefficiencies and duplication of efforts.

Due to the lack of a European interoperability infrastructure interconnecting all public authorities relevant for maritime surveillance, several initiatives have emerged within every User Community over the past years to remove barriers to cross-border interoperability. This means that in most User Communities, EU-wide systems are already in place, supporting their day-to-day activities e.g. SafeSeaNet for vessel traffic monitoring and information. The next step is to remove the barriers between User Communities that prevent information from flowing between them.

In December 2009, to make information sharing across User Communities a reality, the European Commission adopted a communication "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain" [9]. In 2010, the European Commission put forward a six-step Roadmap towards the Common Information Sharing Environment (CISE) [6]. Since then, several initiatives have been set into motion to achieve CISE. Among these initiatives are two pilot projects on integrated maritime surveillance, namely the MARSUNO pilot project in the Northern Sea Basins; and the BlueMassMed pilot project in the Mediterranean Sea Basin. The reports of these pilots were extensively used as input to this document.

EU Ministers for Maritime Affairs have instructed the institutions in the Limassol Ministerial Declaration in 2012 that CISE should be operational and active by 2020. Through the Declaration, the Council expressed support for the integration of maritime surveillance through CISE, and recognised its potential to become an effective and cost-efficient way of safeguarding EU interests [10].

The architecture visions document belongs to step 4 of CISE's roadmap and it will support the Member States' Expert sub-Group on the Integration of Maritime Surveillance to identify CISE's preferred architecture vision. The figure below shows that the visions are the main input to the design activity of the development of CISE's supporting framework. This document builds on the study on the current IT landscape [8] and the pilot projects on maritime surveillance.

[3] It should be noted that the scope of Common Information Sharing Environment (CISE) extends to all sea basins with EU interest, as some EU Member States have overseas regions, such as France.

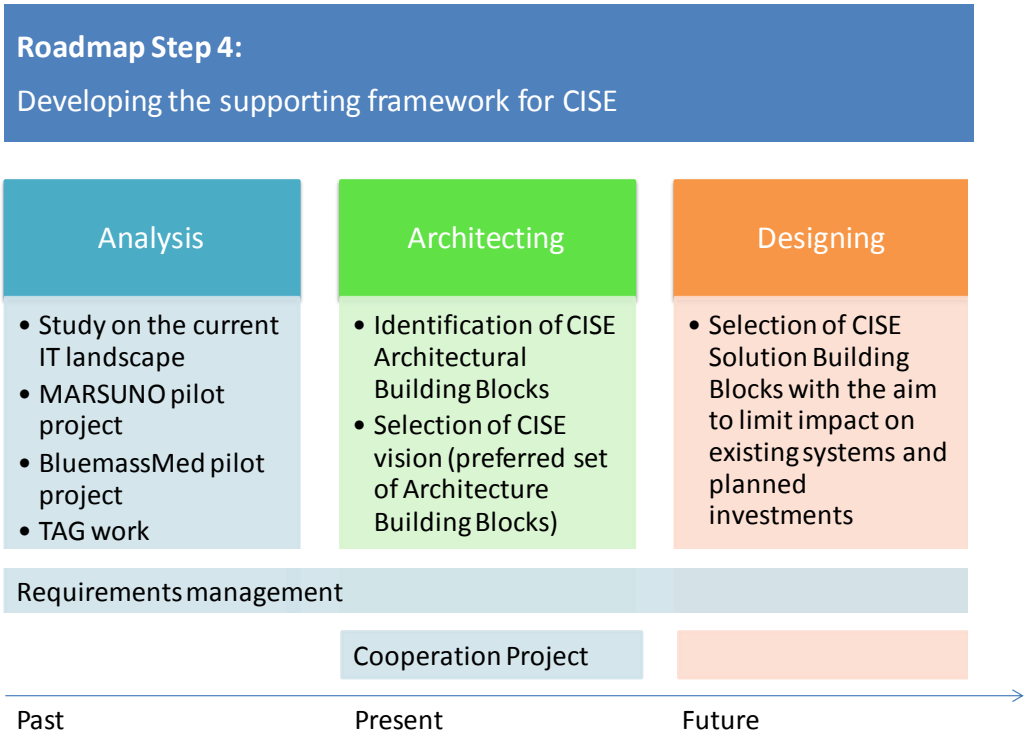


Figure 2 Step 4 of CISE's roadmap

This document benefited from the work carried out by the following on-going initiatives:

- the Cooperation project between several Member States has as its main objective to detail the first set of use cases and supporting information services, agree on common data models, define common reference data and describe common data classification levels for CISE, and as such supporting the identification of CISE's vision.
- the CISE Impact Assessment assessed the legal, economic, social and environmental feasibility and impact of using different legal instruments to remove barriers blocking information exchanges between User Communities.
- the costing of the architecture visions was carried out in a different work stream [11] and then integrated in this document.

1.2. Purpose

The purpose of this document is to present alternative target architectures for CISE, conceptualised following the approach explained in detail in section 2.1. It is important to note that the building blocks composing each vision do not need to be built from scratch, and that the reuse of existing specifications and systems is preferred. As explained in the roadmap document of 2010: "*Existing systems of the various partners are only impacted insofar as a module must be added to allow the web services to catch the required data*." [6]

As previously explained, the architecture visions are composed of generic building blocks, therefore:

- they do not embrace every detailed aspect of CISE, instead, they focus on those aspects that are relevant for an agreement on CISE's conceptual architecture; and
- they provide a structure for discussing how CISE should be implemented and what are the next steps to ensure that the right architecture is reached, in the most efficient and effective manner.

1.3. Key concepts

For the purpose of the Architectures Vision for CISE, the key concepts provided in this section apply.

1.3.1. What is CISE?

In the context of Integrated Maritime Policy (IMP), there is currently no underlying framework for the sharing of maritime surveillance data across the seven maritime surveillance functions. This is the case because their information systems (at EU, national and regional level) were designed and continue to evolve independently of each other. The CISE initiative intends to create an environment where all maritime surveillance functions can cooperate with one another and share data following a common set of rules.

1.3.2. Architecture Vision in the context of CISE

A unifying architecture vision for CISE is a means to define the architectural building blocks of CISE at Legal, Organisational, Semantic and Technical levels, thereby contributing to the development of an Integrated Maritime Policy.

1.3.3. Architecture Building Blocks

Every architecture vision is composed of a set of Architectural Building Blocks. These building blocks describe the different aspects of each vision and how CISE's information systems will be made available by Member States and EU initiatives. These building blocks are (technical) solution neutral but typically describe required capabilities, and shape the specification of Solution Building Blocks. For instance, if a Messaging Protocol is an Architectural Building Block, the SSN XML Messaging is a Solution Building Block.

1.3.4. CISE Information Service

A CISE information service makes available, to CISE participants, raw, consolidated or fused data in one or several given geographical areas and/or functions.

1.4. Why are architecture visions needed?

The architecture visions described in this document are intended to support the Member States' Expert sub-Group on the Integration of Maritime Surveillance in identifying the preferred set of building blocks of the Common Information Sharing Environment (CISE). These building blocks, also referred to as Architecture Building Blocks, are solution-neutral. Instead of prescribing specific technologies, the visions specify Architectural Building Blocks which allow for different kinds of Solution Building Blocks to realise them.

As explained in CISE's roadmap: "*Existing and planned systems shall be duly taken into account while developing the CISE. This process shall also not hinder the development of existing and planned sectorial information systems, as long as the need for interoperability enabling information exchange with other systems is taken into count (*...)") [6]. In the same spirit, MARSUNO clarifies, in its final report, that *"(...) an optimised information sharing environment should not replace existing systems but should provide guidelines for their evolution as well as a common interoperability framework in order to improve the global efficiency at a European level and to reduce the cost of new functionalities (...)"* [4].

Having the above in mind, once the preferred target architecture model of CISE is identified, the specific Solution Building Blocks for CISE will be chosen, taking into account the need to:

- minimise the impacts – if any - on operational information systems[4]; and
- protect planned future investments e.g. the Single Window projects to be carried out in the European Union Member States, to implement *Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports* [7] , as well as other existing EU initiatives.

1.5. Why several architecture visions?

At the time of writing, multiple stakeholder perspectives coexist as to how CISE should be set up. This document describes each one of these alternatives as architecture visions. Since no consensus has been reached on one single Vision that accommodates the specific situations and needs in terms of architecture of each Member States, this document also contains a "Hybrid Vision", which provides more flexibility and choice of architectural solution to the Member States (see table below). Conceiving clear, vivid and well-structured architecture visions for CISE is important as a decision-making tool for setting up a commonly identified and consequently agreed-upon direction for the CISE project as a whole.

In parallel, the architectural visions are being analysed in an impact assessment study, which assesses the visions' impact in terms of their legal challenges, as well as their economic, environmental, and social impact. The outcome of this assessment is of critical importance for the future development of CISE, as this influences CISE's ability to accommodate maritime functions with different regulatory frameworks and technological maturity.

This document defines the architecture visions for CISE by drawing inspiration from existing related initiatives and from past studies e.g. the study on the current maritime surveillance IT landscape [8] and the CISE pilot projects (MARSUNO [4] and BlueMassMed [5]). The recommendations for CISE from these two pilot projects can be found in Annex 3 , where a mapping is made between the recommendations of the pilot projects and the visions presented here. The table below shows the name of the architecture visions considered in this document and their source.

[4] It is, nevertheless, understood that authorities at any level are autonomous in proceeding with any additional upgrades of their system at any time to improve the quality of their maritime awareness picture and service provision.

Table 1 Architecture visions

ID.	Architecture Vision name	Source/ Stakeholder Perspective
Core	**Multiple Providers of CISE Services at National level (+ EU initiatives)** The CISE Core is not a vision like the others. The purpose of the CISE Core to describe CISE's minimum viable architecture as a basis for defining the other visions. Therefore, it does not prescribe a governance model. As the minimum required architecture, the building blocks of the CISE Core Vision are also represented in all other Visions.	Inspired by the Large Scale Projects of DG CONNECT and other Trans-National Systems already in operation in the EU.
A	**Multiple providers of CISE Services coordinated by User Communities (+ EU initiatives)** This vision proposes a governance model centred on User Communities. Ideally each User Community should have a single service provider at national level and one or more EU led initiatives. Consequently, the integrated maritime awareness pictures available in CISE are divided by User Community.	Resulted from discussions in TAG
B	**Multiple providers of CISE Services coordinated by Member States (+ EU initiatives)** This vision proposes a governance model where each Member State appoints an authority to manage which CISE services are delivered by one or multiple service providers. CISE services are also be provided by EU led initiatives. As in Vision A, several integrated maritime awareness pictures coexist, but they are no longer divided in User Communities.	Inspired by the BlueMassMed pilot [5] and MARSUNO pilot [4] with some modifications based on feedback received from the TAG.
C	**Single national providers of CISE Services (+ EU initiatives)** This vision proposes a governance model where each Member State appoints an authority to manage which CISE services are delivered. Unlike vision B, each Member State has a single service provider of CISE services. CISE services can also be provided by EU led initiatives. Unlike visions A and B, a single integrated maritime awareness picture can be offered per Member State. Sea basin authorities can also be set up to provide sea basin level services (variant of vision C).	Inspired by the BlueMassMed pilot [5] and the MARSUNO pilot [4].
Hybrid	**Merge of Visions A, B and C** The hybrid vision proposes a two-level governance model: **1st level:** CISE Contact Points at Member State level to manage the catalogue of CISE services of each Member State. These are the services belonging to, and provided by, the Member States. **2nd level:** CISE Contact Points at EU level to manage the catalogue of CISE services of each User Community. These are the services belonging to the User Communities and provided by EU led initiatives, usually, under the supervision of EU agencies. The Member States are involved in the governance of these initiatives. The hybrid vision makes it possible for Member States to decide whether to nominate a single provider of CISE services or multiple ones.	Resulted from discussions with the Member States

It should be noted that the CISE core is not a vision like the others. The purpose of the CISE Core is to describe CISE's minimum viable architecture as a basis for defining the other visions. Therefore, it does not prescribe a governance model. As the minimum required architecture, the building blocks of the CISE Core Vision are also represented in all other Visions. The building blocks of CISE's core were derived from the list of principles in Chapter 4, the list of requirements in Chapter 5, other relevant EU level Large Scale Projects and the analysis of the CISE pilot projects on integrated maritime surveillance (refer to Annex 3).

Aside from the CISE Core, each architecture vision proposes a different collection of building blocks for CISE. To allow for easy comparison of visions, each alternative is described in a structured template and assessed based on commonly agreed criteria - please refer to section 6 Architecture visions of CISE. This criteria includes both quantitative (e.g. CISE requirements coverage and cost assessment) and qualitative assessments (e.g. assessment of long-term benefits) for each vision.

1.6. Outline

Chapter 1 is the introductory chapter explaining why architecture visions are needed, as well as the context and purpose of this document.

Chapter 2 explains the approach that was taken to conceptualise the architecture visions; it also describes how the European Interoperability Framework (EIF) of the EU programme for Interoperability Solutions for European Public Administrations (ISA) [12][5] is used to structure each vision according to organisational, semantic and technical levels. The legal level is not part of the scope of this document.

Chapter 3 aims to provide a high level understanding of each vision's interoperability agreements by providing an overview of each vision. The focus of this chapter is on the essential characteristics of each vision, and the differences between them. This chapter also explains how the preferred architecture vision will be identified.

Chapter 4 lists all identified and documented principles for CISE.

Chapter 5 lists all identified and documented requirements for CISE. This is a work in progress catalogue that will continue to be updated throughout the lifecycle of CISE.

Chapter 6 describes the core CISE building blocks and each architecture vision in detail. Refer to section 6.1 for a detailed explanation of how each vision is unfolded and the selection criteria for the preferred architecture model.

The **last chapter** contains the bibliography used in this document. The **annexes** at the end of this document provide the following information:

- Annex 1 - an extensive glossary of terms and abbreviations;
- Annex 2 - a summary of the as-is state in maritime surveillance;
- Annex 3 - a table of recommendations from CISE pilot reports;
- Annex 4 - the detailed requirements coverage analysis;
- Annex 5 - explanation of how to provide comments on this document.
- Annex 6 - a description on how the EU led initiatives fit into the hybrid vision.

[5] ISA sponsors the CISE project, as it aims at facilitating efficient and effective digital interaction between public administrations in Member States.

2. ARCHITECTURE VISIONS CONCEPTUALISATION

2.1. Approach

The architecture visions described in this document could have been created following a classic top-down approach, i.e. starting from the requirements of CISE, or a bottom-up approach starting from the analysis of the existing information systems, which will share information through CISE. However, the CISE visions were conceptualised using both the top-down and bottom-up approaches as inspiration in order to capture the views of multiple stakeholders and to identify the building blocks of each architecture vision. This approach is referred to as the hybrid approach and it takes into account multiple sources of input, as it can be seen in the figure below [13].

Top-down approach	Hybrid approach	Bottom-up approach
Suitable for situations where the requirements are very well-defined and there is a clear organisational structure so that gradual zooming in is possible.	Takes into consideration known requirements, existing systems, planned investments, and results of pilot projects; whereby a mix of zooming in and out is used.	Suitable for situations where the number of existing information systems is limited so that gradual zooming out from them is possible at a relative low cost.

Figure 3 Approach to conceptualise the architecture visions

After defining the building blocks of each vision, every vision was described using a template structured based on the EIF of the ISA programme [3]. ISA's interoperability framework is *"an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services"*. This framework describes four levels of interoperability for implementing cross-border/cross-sector services.

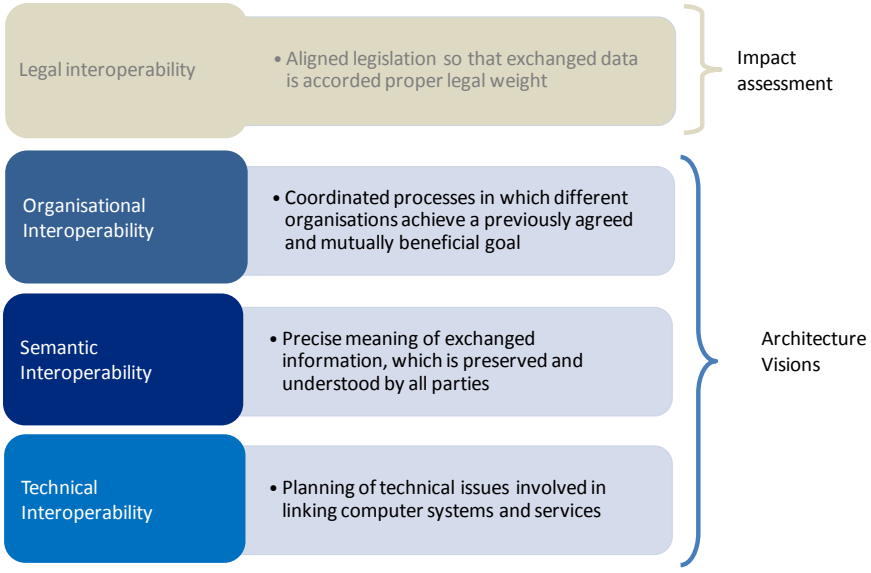


Figure 4 Interoperability layers of the European Interoperability Framework

As shown in the figure above, this document does not touch upon the legal interoperability layer. The policy options are being analysed as part of CISE's impact assessment and are therefore not addressed in this document. Nevertheless, the architecture visions are complementary to it. The figure below maps the different layers of the EIF to the policy options and the architecture visions.

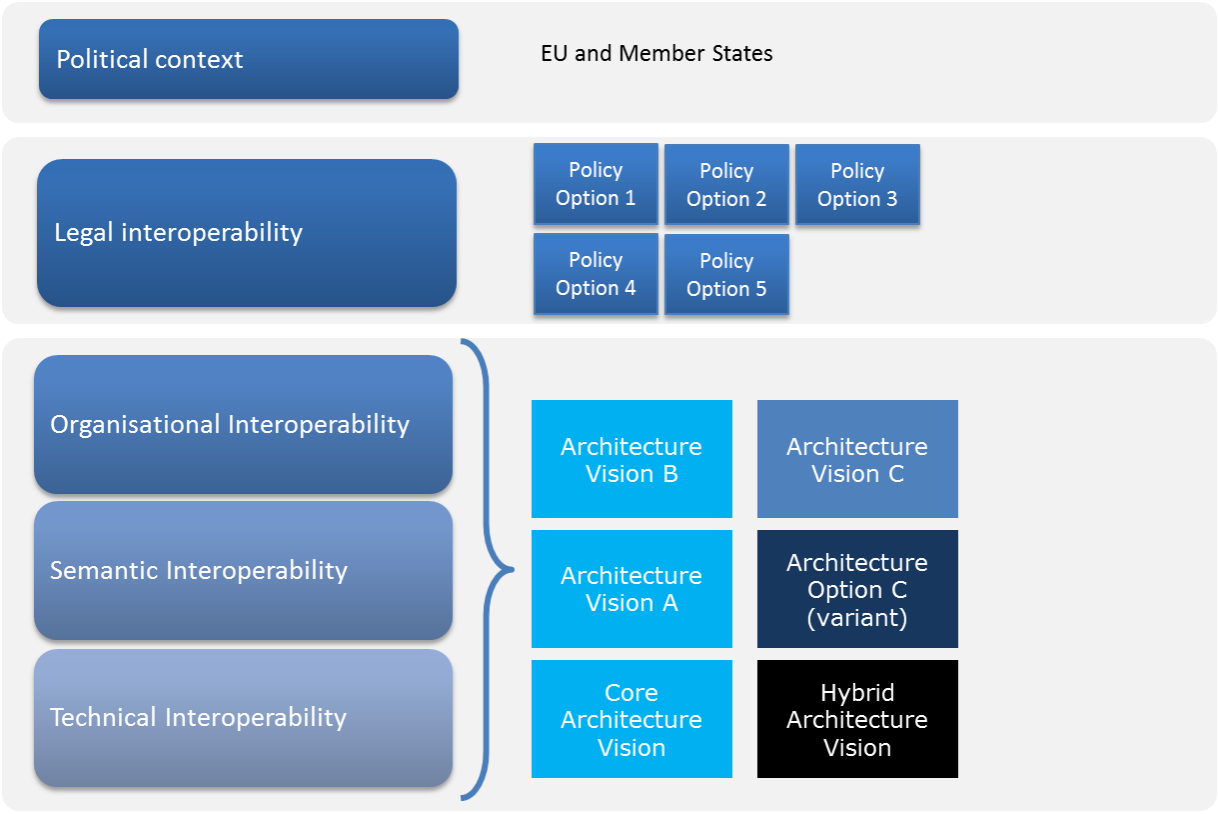


Figure 5 EIF mapped to policy options and architecture visions

2.2. How are the architecture visions structured?

As explained in the EIF, interoperability agreements are the means through which participants of large ICT projects formalise cooperation with one another. These agreements aim at leaving each Member State with maximum internal autonomy, minimizing the impact on their operational systems, while creating an area of cooperation where information can flow without barriers to interoperability.

CISE will respect the general principles of the European Union law and in particular the principles of subsidiarity and proportionality. This means that within the context of CISE no action, except in the areas that fall within its exclusive competence, at European level will be performed, unless it is more effective than action taken at national, regional or local level. The involvement of the institutions must also be limited to what is necessary to achieve the objectives of CISE.

Once agreed by all CISE participants, the architectural building blocks become interoperability agreements to remove barriers to information sharing across borders and sectors. Having this in mind, the architecture choices are structured around three main questions at organisational, semantic and technical levels:

A. What is the desired level of organisational interoperability among CISE participants?

B. What is the desired level of semantic interoperability among CISE participants?

C. What is the desired level of technical interoperability among CISE participants?

Each one of these questions will be explained in more detail in the following paragraphs.

A. What is the desired level of organisational interoperability among CISE participants?

Organisational interoperability lays the foundation for CISE participants to work together and achieve their mutually agreed goals. For organisational interoperability to happen, agreements must be reached to crystallise consensus on:

- CISE's governance model: this model defines how CISE's service catalogues are managed. It can be done by splitting responsibilities by organisational levels, by User Communities, or a combination of these two.

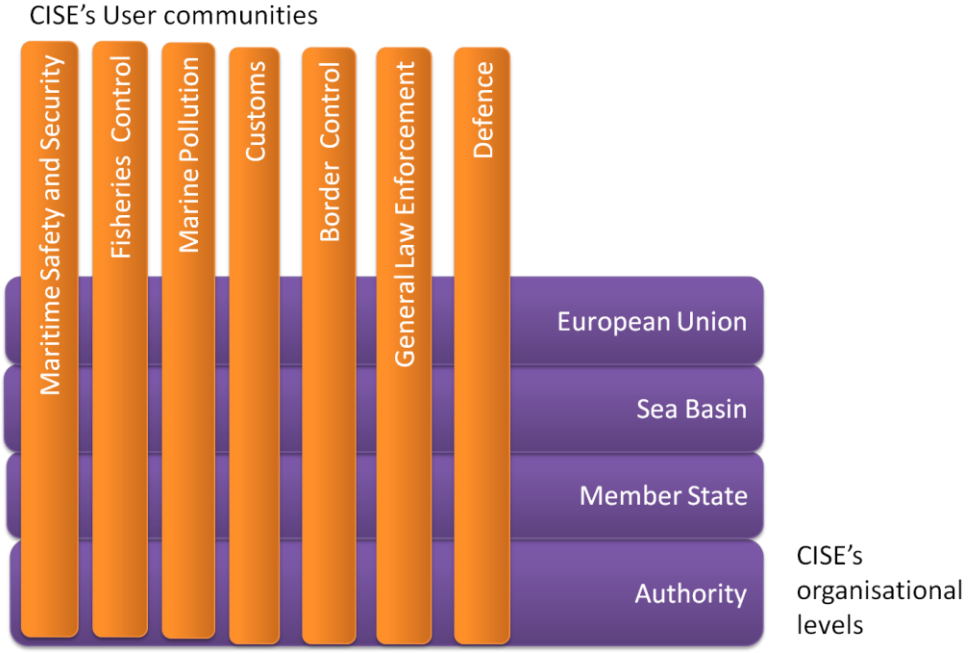


Figure 6 Organisational levels and User Communities

- CISE's service delivery model: this model defines how CISE services are delivered. CISE services can be provided by EU led initiatives, Sea Basin authorities and Member State authorities. At national level the following two basic models can be used:
  - A single authority that collects information from the several sources and redistributes it (through a set of CISE services);
  - Multiple authorities providing CISE services.
- CISE's integrated maritime awareness picture model: this model defines the scope of the integrated maritime awareness pictures. The scoping options are:
  - Public authority scope: several maritime awareness pictures coexist restricted to the scope of the information held by the public authority providing this service. The information contained in these pictures is not oriented towards the specific needs of User Communities;
  - User community scope: several maritime awareness pictures coexist restricted to the scope of the information held by the public authority providing this service. The information contained in these pictures is oriented towards the needs of User Communities;
  - Geographic: several maritime awareness pictures coexist oriented towards the geographical scope of the Member States and possibly Sea Basins providing them.

Figure 7 provides an overview of all the interoperability agreements present in each vision. Since the visions mostly differ in organisational agreements (rather than semantic or technical), Figure 8 zooms in on how the organisational interoperability agreements differentiate the visions.

B. What is the desired level of semantic interoperability among CISE participants?

In the context of semantic interoperability, agreements focus on the meaning of datasets and their relationships. In practical terms, this means agreeing on a common "CISE language" and to ensure that information is understood in the same way by the several CISE participants of the seven User Communities. For semantic interoperability to happen, agreements must be reached to crystallise consensus on the following set of specifications:

- A common information exchange model. This encompasses specifying a common data dictionary, common controlled vocabularies (e.g. code lists and other reference data) and the semantics (e.g. the meaning) of the data payload(s) which will be exchanged within the services' messages. The semantics of CISE shall build upon and not modify existing sectorial semantics;
- Data classification levels and access profiles as explained in CISE's roadmap: "In order to facilitate cross-sectorial information exchange, User Communities should develop a common approach when attributing classification levels" [14];
- Catalogue of datasets and information services.

The building blocks at the semantic level are common in the CISE Core and all consequent visions. The governance of the specifications and standard-like artefacts produced by CISE at semantic level could be sustained by a standardisation body e.g. UN/CEFACT, W3C, CEN, etc. In this case, their governance would be independent from CISE's governance model.

C. What is the desired level of technical interoperability among CISE participants?

At technical level, CISE's participants define how services will be developed in technical terms. These services are accessible through technical interfaces using a messaging interaction model. CISE has many similarities to most EU-wide information exchange projects such as CCN/CSI of TAXUD [15], the Large Scale Pilots of DG CONNECT [16], VIS and SIS II of DG HOME [17], etc. At the time of writing, several European Commission led initiatives are on-going to harmonise the Pan-European information systems. These include ISA's action "Towards a European Interoperability Architecture" [18] and e-SENS ('Electronic Simple European Networked Services') of DG CONNECT [19]. A message exchange will happen when CISE participants share information on request or when they communicate notifications. CISE participants will play the role of "Service Provider" when sharing data through a service and of "Service Consumer" when calling a service to use data. For technical interoperability to happen, agreements must be reached to crystallise consensus on:

- Specifications: Messaging protocol and potentially the service discovery specifications and correlation and fusion rules;
- Reference implementations: Gateway (implements the messaging protocol specifications for data exchange), node (includes the gateway and correlation and fusion rules) and service discovery coordinator. The use of the reference implementations is optional.
- Services: Catalogue of CISE services.

At technical level, the main difference between the visions lays in the choice to set up a gateway for message exchange or a node (which in addition to the gateway's functionality also offers correlation and fusion capabilities). The use of a node is linked to decisions made in the organisational level, as it is more beneficial to choose a node e.g. when services are provided by one single provider on behalf of multiple authorities.

Independently of the choice made, the preferred architecture will only prescribe the minimum required number of building blocks agreed by all participants, it is left to the will of the public authorities and/or Member States to add more building blocks if they wish to do so.

The governance of the specifications and standard-like artefacts produced by CISE at technical level should be sustained by a standardisation body, such as the ones mentioned above. If this happens, their governance will be independent of CISE's governance model.

Figure 7 Summary of building blocks and interoperability agreements provides an overview of all the interoperability agreements present in each vision in the above mentioned areas – organisational, semantic and technical.

3. HOW TO COMPARE THE ARCHITECTURE VISIONS

3.1. Understanding the different architecture visions

CISE aims to eliminate existing barriers to interoperability between User Communities. These barriers can only be removed when CISE's building blocks are defined and agreed among all participants, at which point they become interoperability agreements at organisational, semantic or technical level. Each architecture vision proposes a different set of building blocks, and therefore interoperability agreements. The figure below gives an overview of the interoperability agreements proposed in each architecture vision.

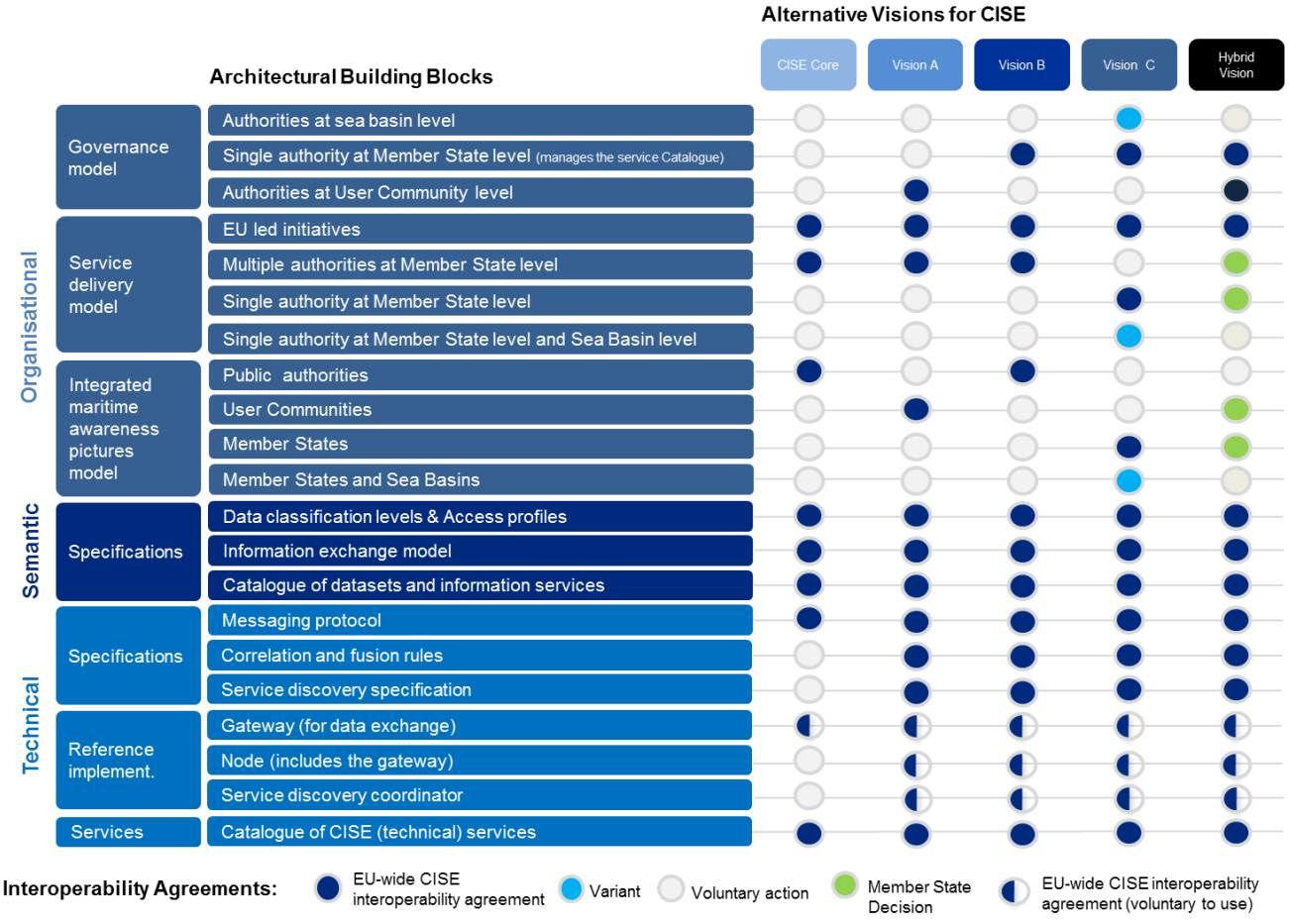


Figure 7 Summary of building blocks and interoperability agreements

Please note that the above mentioned reference implementations can be provided to CISE participants as the standard, against which other implementations can be compared. The use of the CISE reference implementations is optional.

In addition to the above set of interoperability agreements, a supplementary set of real-time collaboration tools may be provided as part of CIE to allow CISE participants to easily interact with one another. This is common to all visions.

A more detailed explanation of the building blocks and interoperability agreements, shown in the figure above, is provided in the next sections.

3.2. How different are the architecture visions?

As shown in Figure 8, visions A, B, C and the hybrid vision require the same set of interoperability agreements at the semantic and technical layers. This is the case, because they respond to the same basic business requirements. The main differences can be found in the organisational layer. At this layer, each vision gives a different answer to the following three fundamental questions:

1. How could CISE's integrated maritime awareness picture be created?
2. How could CISE be governed?
3. By whom could CISE services be delivered?

The picture below depicts the characteristics of the architecture visions by pairing the questions above.

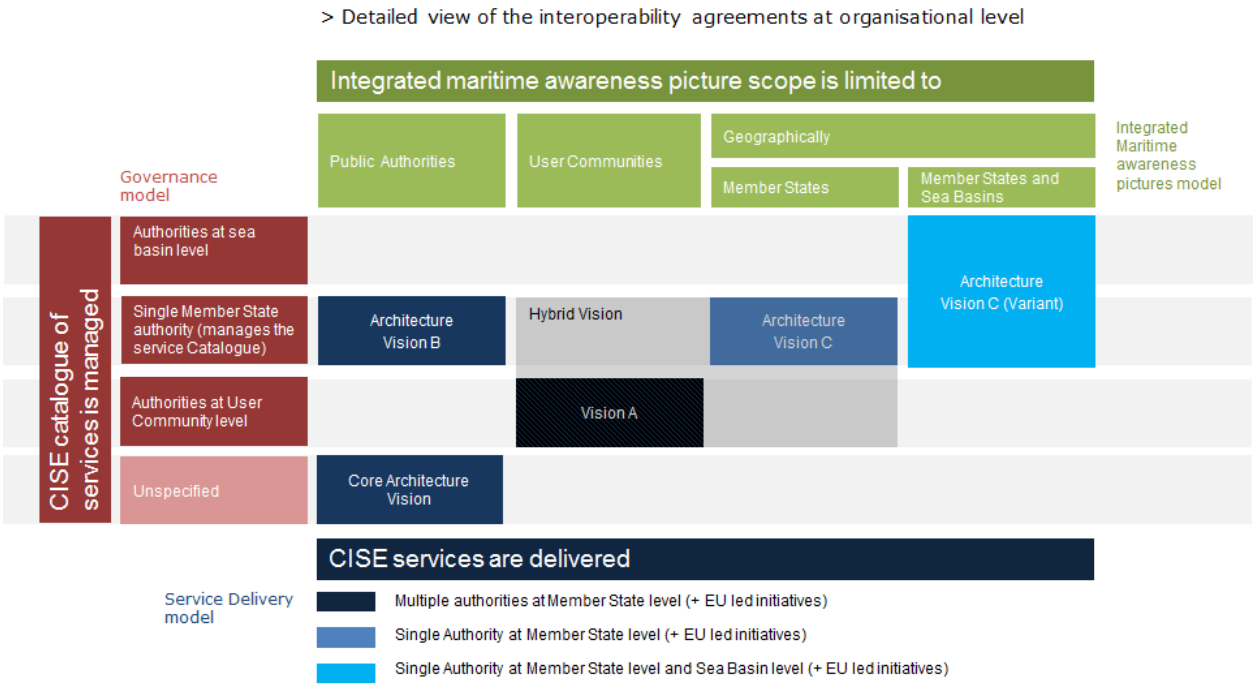


Figure 8 Architecture visions

As an example, the figure above shows that in vision B:

- The integrated maritime awareness picture that can be provided is limited to the scope of services provided by a given authority (top row). This does not exclude the possibility of a national public authority being mandated to offer a national integrated maritime awareness picture by collecting information from all other national public authorities. This choice, as all others, also includes EU led initiatives (e.g. EU Agencies or European Commission central systems), allowing them to manage and deliver their own services;
- Each Member State must appoint a single authority (e.g. inter-ministerial cooperation) to manage the national catalogue of services (left column); and
- Services are offered by individual authorities within a Member State (bottom row).

3.3. How will the architecture visions feed into the debate about CISE and the next steps?

The template used to describe the architecture choice contains quantitative and qualitative selection criteria. The aim of this document is not to conclude on a preferred architecture vision but to feed into the debate and provide stakeholders with the necessary information to make a fact-based decision on the best way towards CISE. It will be used, along with the results of other studies such as the on-going impact assessment, to support future actions of the Commission related to the Integrated Maritime Policy.

Once a preferred architecture vision has been agreed on, several approaches may be considered when creating the implementation plan. A good understanding of the dependencies and lifecycle of the several Solution Building Blocks will be required, as well as the readiness of the participants in CISE's first phase. The implementation of the preferred architecture will be done in iterative steps (as opposed to big bang) and will require a roll-out plan. The Solution Building Blocks and stakeholders to be included in the different steps, and the exact sequence of these steps, are not yet decided. Following this iterative approach, MARSUNO proposed the following natural convergence towards CISE in their final report:

"It would be too much to imagine that creating a new European system could emerge from nothing. Administrations, nations, community of users already have each of them their own organisation, priorities and systems (maritime surveillance systems, data bases, risk analysis tool) and these actually work satisfactorily. Nevertheless it has been identified that a better interoperability, a better sharing of information, mainly automatic, cross sector and cross border, between administrations in charge of maritime surveillance will enable them to create a better Maritime Situational Awareness and improve their management of risk, their knowledge of maritime events and eventually their efficiency. A well-defined and common framework can be sufficient to entail a natural convergence towards an optimised CISE with time. Indeed, the medium lifetime for an information system is about three years. Each new update can be a step toward a more interoperable system of systems by using:

- *the last version of adopted common data model defined at EU level by a cross-sectorial expert group,*
- *the last version of adopted common standards and rules regarding interfacing between national systems,*
- *legal environment and if possible legal umbrella at the EU level."* [4]

4. PRINCIPLES OF CISE

CISE must respect the general principles of the National and European Union law e.g. International Agreements binding User Communities managing data belonging to third parties. This means that within the context of CISE no action, except in the areas that fall within its exclusive competence, at European level will be performed, unless it is more effective than action taken at national, regional or local level. The involvement of the institutions must also be limited to what is necessary to achieve the objectives of CISE; the content and form of the action must be in keeping with the aim pursued.

In addition to the general principles of European Union law, CISE also has its own set of specific principles. They provide for a high level design rationale that must always be taken into account when creating, changing or removing anything in the context of CISE.

The European Commission's requirements management tool is used to manage principles.

The principles of CISE are listed in the table below.

Table 2 CISE Principles

ID	Title	Description
P1	CISE must allow interlinking any public authority in the EU and in the EEA involved in maritime surveillance.	The objective of CISE is to improve maritime awareness by improving the maritime public authorities' abilities to monitor, detect, identify, track and understand occurrences at sea in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge. Stakeholders (user communities, member states, public authorities, EU agencies ...).
P2	CISE must increase maritime awareness based on need-to-know and responsibility-to-share principles.	The need-to-know principle, as established in the EU data protection rules, is the idea of public authorities needing and being able to access information from other communities in order to enhance their integrated maritime awareness picture. The responsibility-to-share principle promotes the idea of public authorities having an obligation to share information with other communities, following appropriate access rights policy, to support them in their decision-making processes by contributing to a more complete integrated maritime awareness picture. This will need to be defined in the relevant sectorial legislation.
P3	CISE must privilege a decentralised approach at EU-level.	CISE must be based on a decentralised approach, meaning that public authorities should be able to exchange information, based on common standards, while respecting access rights.
P4	CISE must allow interoperability among civilian and military information systems.	CISE must support interactions between civilian and military systems to allowing for the most complete integrated maritime awareness picture.
P5	CISE must allow interoperability among information systems at the European, national, sectorial and regional level.	Improving maritime awareness requires making information available to maritime authorities that previously encountered barriers in trying to obtain that information. CISE participants must be able to access information from national, regional, sectorial and European authorities in a flexible way.
P6	CISE must privilege reuse of existing tools, technologies and systems.	CISE must build on prior work and must favour the reuse of existing tools, technologies and systems as much as possible.

ID	Title	Description
P7	CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance.	CISE must be able to handle all types of information relevant to maritime information, including non-sensitive, sensitive and highly-secure information.
P8	CISE must be system neutral.	All public authorities should have equal participation in CISE, without requiring them to modify their own internal structures and systems (apart from what may be required to implement as minimum commonly agreed elements of CISE).
P9	CISE must make it possible for information providers to change their service offering.	Information providers will be able to change the services they offer, according to a commonly agreed notification procedure.

5. REQUIREMENTS OF CISE

The tables below describe the requirements for CISE. Each requirement is defined by an ID, a title and a description. They are categorised using the below scheme:

- **Information sharing**: these describe the basic information workflows in terms of requesting and subscribing to information and notifications.
- **Information discovery**: information discovery details how CISE participants can find information using CISE.
- **Information assurance**: information exchanged through CISE will give the receiver the ability to assess the value of the information.
- **Information security**: CISE must be able to handle non-secure, secure and highly sensitive information.
- **Collaboration between CISE participants**: CISE participants must not only be able to exchange information, they must also be able to (virtually) collaborate and get in touch with each other.
- **Organisational aspects**: CISE must be managed, requiring certain organisational functions.

The requirements come from various sources, including the MARSUNO and BlueMassMed pilot projects and will be kept up-to-date at all stages in the realisation of CISE. The requirements will also be revised on the basis of conclusions from the on-going cooperation project. When adding or changing requirements, this should always be done in respect of the CISE principles – these should always hold true.

The European Commission's requirements management tool is used to manage requirements.

The requirements of CISE are listed in the table below.

5.1. Sharing of information

Table 3 CISE Requirements on sharing of information

ID	Requirement	Description
SI1	CISE must facilitate increasing maritime awareness by authorities at national, Sea Basin, User Community or in the EU maritime domain level.	CISE must facilitate more than exchanging "raw" information; the value of CISE lies in improvements in the decision-making of public authorities by bringing cross-border and cross-sector information together. CISE is meant to fill the information gap necessary for any relevant authorities at any level to enhance their existing or to create new awareness pictures. Such pictures may serve both operational and policy making/governance needs at local, regional, national, Sea Basin or EU level.
SI2	CISE must support sending information upon request, subscription or spontaneously.	A CISE participant must be able to share its information with any other participant. There are three scenario's in which a participant can send information: • As a response to a request that was sent by another participant; • A participant can send information to all participants that are subscribed to one or more of its services; and • As a spontaneous sharing of information. This scenario allows participants to share information they believe is relevant, even if it was not requested. The purpose is to help improve situations in which other participants might not be aware that the information exists or that they need it.
SI3	CISE must support sending notifications upon subscription or spontaneously.	A CISE participant must be able to send a notification. A notification is used to inform other participants of an event. Events can relate to the maritime domain (e.g. a collision, an oil-spill, a suspect ship entering European waters, etc.) or to anything related to the sender of the notification (e.g. a notification to inform about a service that is or will be temporarily unavailable, the availability of a new information or data, etc.). Sending notifications spontaneously can be done to one or more participants at the same time using access profiles (IS1).

ID	Requirement	Description
SI4	CISE must support requesting information.	A CISE participant must be able to request information from any other participant. This basic information sharing scenario supports situations in which participants can use information from others to improve their own actions and decision making.
SI5	CISE must support subscribing and unsubscribing to information at any time.	In case a CISE participant knows that another participant has useful information that it frequently needs, it can subscribe to a service of that participant. The subscription request is sent once, but afterwards, the subscriber will continue to receive information from that participant with frequency defined by the information provider (e.g. daily, monthly, as soon as there is new information, etc.). A participant can also unsubscribe from any existing subscriptions if they no longer wish to receive the information.
SI6	CISE must support subscribing and unsubscribing to notifications at any time.	Similar to subscriptions to information, participants can also subscribe to notifications. This allows them to remain aware of events in the maritime domain or of events related to any participant, without having to receive a set of information to process.
SI7	CISE must support requesting or subscribing to information without knowing who the provider of the information is.	In order to reduce situations in which authorities are unable to make a sound decision due to a lack of information and not knowing where this information could be requested, CISE must support requesting information without first having to know whom to contact. A multicast or broadcast system supports sending requests to multiple authorities at once. Authorities that have the requested information can then reply. CISE information requests can for instance be used to request information on (these examples are non-exhaustive): • A vessel. Information about a vessel must be able to be requested using any of the existing vessel identification means (a unique ID, a name and country, etc.). • An area. Information about a particular area can be requested using a commonly agreed geographic identification system. • An action by a maritime authority (any maritime intervention, possibly in response to an event).

ID	Requirement	Description
SI8	CISE information requests can specify the time-frame for which the information is requested.	There is no time limitation on information shared through CISE; it can be historical or current. CISE participants should be able to request information from a specific period.
SI9	CISE must rely on a common data model for information exchanges which is as language-neutral as possible.	Information shared through CISE must be made available using a common data model so that all CISE participants can understand and use the information. This common data model must be language neutral, meaning that it should not favour any of the languages of the European Union and that it can be used with any of the languages of the European Union. During the release migration process, the interface must support data models X and X+1 (this applies to both minor and major releases).
SI10	CISE must rely on a common messaging protocol for information exchanges.	CISE participants must use a commonly agreed messaging protocol to exchange information in support of transport characteristics such as integrity and reliability. During the release migration process, the interface must support protocols X and X+1 (this applies to both minor and major releases).
SI11	CISE must rely on common standards for information processing.	To promote a common understanding of information relevant to maritime surveillance, CISE must foster the use of common standards to interpret and process exchanged information (by performing e.g. aggregation, correlation or fusion on the information). This is e.g. important to build an integrated maritime awareness picture.
SI12	CISE participants must be able to approve information requests or subscriptions manually.	Typically, everything is done automated for effectiveness. But sometimes manual approval might be needed. This is an exception, however.
SI13	CISE must support exchanges of varying file sizes, including large files.	Information exchanges must support exchanging files of varying size. This is necessary to support the exchange of large satellite images and maps for example. The maximum supported file size can only be established as part of a technical analysis of relevant file sizes however.

ID	Requirement	Description
SI14	CISE participants providing information must provide statistics per service on information exchanged through CISE.	A CISE participant exposing services should offer statistical information on that service's usage. This information is not only useful for the information provider, but also for the information consumer. Furthermore, this allows for a performance analysis of the service and can provide insights in how to best evolve the service. CISE participants must have access to the statistical information on exposed services. This provides them with insights on the performance of a service and supports them in making a sound decision on if and how to use the service.

5.2. Discovery of information

Table 4 CISE Requirements on discovery of information

ID	Requirement	Description
DI1	Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants.	CISE must try to hide as much organisational, semantic and technical complexity from its participants as possible. Organisational complexity is an important barrier to information sharing that cannot be reduced or eliminated by mere technical means. An organisational change, by providing one or more points of access for a larger group of CISE participants, will support other participants in discovering the services of such a group.
DI2	CISE must allow retrieving contact information about CISE participants.	The maritime domain is characterised by a large number of varied stakeholders. To promote collaboration, CISE must provide a means to look-up contact information for the involved stakeholders so that they can contact each other more easily than today. A contact directory, a "phone-book", to look-up contact details can support this.
DI3	CISE must allow looking up what information CISE participants can provide and how they can provide that information.	To allow CISE participants to discover information more easily, CISE must provide a means to look-up what information is available from which CISE participant. By having an overview of what information is available through CISE; participants can more easily discover information to help them improve their maritime awareness.
DI4	CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate.	The usage details of the services exposed through CISE by each participant CISE should be documented and be made available to all participants. This documentation allows participants to assess more easily of if the offered services are useful.

ID	Requirement	Description
DI5	CISE must allow verifying if the services offered by CISE participants are available.	CISE participants must be able to verify if any of the services exposed through CISE is available. If a participant depends on a service to make decisions related to an event in the maritime domain, it must be able to verify the availability of the service so that it can take corrective actions if the service is not available.

5.3. Information assurance

Table 5 CISE Requirements on information assurance

ID	Requirement	Description
IA1	CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value.	A confidence value is used to indicate the quality of and the trust in the information shared through CISE. The confidence value is an opinion, which is why the provider of the confidence value also needs to be identified in the information exchange. The combination of the confidence value and its provider supports the receiver of the information in making its decision as to use the information or not.
IA2	CISE information requests must include a priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value.	Some requests or notifications will likely have a higher priority than others. For example, in the case of a collision or an oil-spill, immediate action is required and any information requests or notifications should be treated first by all involved CISE participants. The priority level is used to indicate the urgency of the request.
IA3	CISE information exchanges must contain relevant characteristics about the information.	To allow CISE participants to adequately use information received through CISE, the information exchanges must describe the characteristics of the information. This meta-information, e.g. the provenance of the information, the time it was collected, updated or sent, it's precision or its level of detail, should be part of the information exchange. Information exchanges must also be able to refer to each other. This supports CISE participants e.g. in providing feedback on information sent or in sending updates to, rectifications of or notifications on earlier exchanged information.
IA4	CISE participants must be able to acknowledge information received.	The provider of information needs assurance as to whether the information was successfully received by other participants in some cases. This might e.g. be the case when the sender is liable for sharing information in due time. Acknowledgements by the receiver can be automated or manual.
IA5	CISE participants must be able to provide feedback on the quality of the information received to the information provider.	To support CISE participants in improving the exchanged information, CISE must support sending feedback on the quality of the information. If the information was e.g. invalid or not up-to-date, the receiver must be able to share this feedback with the provider to allow them to improve their information. The commonly agreed information exchange model must define taxonomy to categorise useful feedback categories (e.g. data invalid, corrupt, etc.).

5.4. Information security

Table 6 CISE Requirements on information security

ID	Requirement	Description
IS1	CISE information exchanges must respect agreed data access rights through access profiles (based on the authority's function).	A CISE information exchange needs to use an access profile. The access profile determines if the requester of the information is entitled to access it. Access profiles are defined at the level of public authorities. This means that the authorities participating in CISE will need to manage its end users to give them access to exchange information. CISE participants do not need to change their internal user profiles, the existence of a mapping to the CISE access profiles is sufficient.
IS2	CISE must support information access rights that can be changed dynamically (respecting a commonly agreed Service Level Agreement (SLA) by the information owner.	Access rights should be managed dynamically to allow for sufficient flexibility in determining who can access what information. The purpose of dynamic access rights is to support crisis situations that necessitate giving temporary access to information that would not be accessible to certain participants under normal circumstances.
IS3	CISE must support information providers providing a service to allow requesting access to their information.	Similar to IS2, this requirement allows CISE to be a dynamic environment. CISE participants can expose a service to allow others, who believe they can benefit from the exposed service but that cannot access it yet, to request access to that service without having to establish a bi-lateral agreement.
IS4	CISE information exchanges are authenticated at the level of the CISE participants and in respect of the CISE access profiles.	Authentication is performed at the level of the CISE participant. This means that it is an authority (in case an information system of that authority) that is authenticated, not an individual end-user within that authority. However, it is likely that different individuals within the same authority have different access rights and privileges. The combination of the authenticated participant and the CISE access profile will determine whether or not an information request will be authorised.

ID	Requirement	Description
IS5	CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret.	CISE interconnects a large number of varied authorities in the maritime domain. This variety necessitates an environment that supports the exchange of non-secure, confidential, secure and highly-secure information. Different channels will be needed to support this requirement; these channels will be linked to the commonly agreed information classification scheme. Over-classification, i.e. classifying information as secure while it is not and could use a non-secure channel, should be avoided. CISE participants, each likely with their own classification scheme, need to map their own internal scheme to the CISE classification scheme when sharing information. The objective is to have a common understanding of what a certain classification scheme means. CISE participants do not need to change their internal classification scheme, the existence of a mapping to the CISE classification scheme is sufficient.
IS6	CISE information requests and subscriptions can use different access profiles to request or subscribe to the same information.	An information exchange needs to support multiple access profiles in that it should be possible for an information provider to identify multiple, different access profiles that are authorised to receive its information.
IS7	CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information.	While confidentiality techniques ensure that the content of an information item or exchange is kept "hidden" from unauthorized individuals, it does not ensure that the information item has not been modified. This is accomplished with integrity techniques. Integrity techniques protect against unauthorized modifications, but they do not protect against unauthorized access and disclosure.
IS8	The communication channels between CISE participants must support non-repudiation.	Non-repudiation means that CISE participants will not be able to deny having sent information to another participant.
IS9	CISE must support interconnecting networks of different security levels, including public and private networks.	CISE must support interconnecting the various networks of existing initiatives, such as CCN/CSI [8] , sTESTA [20] and EU OPS WAN [21]. These networks can use different technologies and security levels.

5.5. Collaboration between CISE participant

Table 7 CISE Requirements on collaboration between CISE participants

ID	Requirement	Description
CO1	CISE must support secure exchange of unstructured information independent of the format the information is in.	Unstructured information is any information that cannot be directly expressed using the commonly agreed information exchange model. An example is a normal file, e.g. a MS Word document. CISE participants must be able to securely exchange information that cannot be exchanged through an exposed service, without any limitations on the format of the file other than those agreed by all CISE participants (see CO2). Example file format include PDF, DOCX, PNG, etc.
CO2	CISE participants should agree on a common set of file formats in order to maximise the usability of exchanged information.	Although CISE does not impose any restriction on the types of information or files changed, it is highly recommended that CISE participants themselves agree on a common set of file formats to be used. Agreement on a set of common file formats will maximise interoperability as participants only need to implement the tools or information systems to process an exhaustive list of file formats. If they do, they are ensured that all received information will be understandable.
CO3	CISE must support secure audio communication.	CISE must provide a means for participants to easily interact with each other using audio tools (e.g. using a computer and a headset),
CO4	CISE must support secure video communication.	CISE must provide a means for participants to easily interact with each other using video tools (e.g. using a computer and webcam),
CO5	CISE must support secure instant messaging.	CISE must provide a means for participants to easily interact with each other using text-based tools (e.g. a chat tool).
CO6	CISE must support secure white-boarding.	CISE must provide a means for participants to easily interact with each other using online collaboration tools such as a white-boarding tool that can be concurrently used by the CISE participants.

5.6. Organisational aspects

Table 8 CISE Requirements on organisational aspects

ID	Requirement	Description
OA1	CISE must support an encompassing governance body that is required to maintain all the commonly agreed elements.	The realisation of CISE will require a number of common elements between the CISE participants. These need to be agreed on by the CISE participants but they also need to be maintained (e.g. the delivery of a new version, the operational oversight on a commonly agreed element, etc.). An encompassing governance body should take on the responsibility of maintaining the commonly agreed elements.
OA2	CISE participants should agree with availability and service levels defined in a bilateral, multilateral or community Service Level Agreement.	If a CISE participant exposes a service, they should also commit to an availability level defined in a (SLA). Defining an SLA is useful if a service is required to deliver high availability or particularly fast transmission of information.

6. ARCHITECTURE VISIONS OF CISE

6.1. How to read the architecture visions

The CISE architecture visions are presented in the following format. An introductory section and a diagram convey the most important elements of the vision.

- "**At a glance**": this introductory section describes the key characteristics of the vision, how it differs from the previous vision, how it contributes to improving maritime surveillance and what building blocks are needed. This section is immediately followed by a diagram.
- **Organisational interoperability**: this section details how:
    - Public authorities are organised in CISE;
    - The organisational agreements that are required to support their interactions; and
    - How CISE would be operated. Operating CISE is described from four viewpoints:
        - Technical management;
        - Application management;
        - IT operations management; and
        - Service desk operations.
- **Semantic interoperability**: this section focuses on how the exchanged information is made understandable to and usable by all maritime authorities and how additional context, such as through aggregation, can be added.
- **Technical interoperability**: this section describes technical interoperability aspects on sharing, discovering and retrieving information. This section goes into detail how authority systems can expose and use services and how information can be securely exchanged. Virtual collaboration is also covered.

An architecture vision also defines the Architecture Building Blocks that need to be further specified in the next CISE initiatives by Member States and sectorial initiatives.

- **Architecture Building Blocks that need to be specified**: this section identifies all elements that will need to be further specified to realise the vision. Definitions of the different components and other technical terms used in this section can be found in the Glossary in Annex of this document.

Each architecture vision is concluded by two sections to support the decision-making process. They provide a qualitative and quantitative assessment of the vision:

- **SWOT analysis**: this section evaluates the strengths, weaknesses, opportunities and threats of the vision compared to the as-is situation. The SWOT analysis provides a qualitative assessment of the vision against the as-is situation as described in [8].
- **Selection criteria**: this section details the vision's effectiveness (improvements to maritime surveillance and requirements coverage), efficiency (short-term costs and benefits) and sustainability (long-term costs and benefits). They provide a quantitative assessment of the vision. The selection criteria are described further in section 6.2.

6.2. Selection criteria

The selection criteria consist of three elements – effectiveness, efficiency, and sustainability.

6.2.1. Effectiveness

In order to understand how each vision contributes to the improvement of maritime surveillance, the assessment of "effectiveness" will look at the different vision's ability to solve the existing problem statements and to meet stakeholder requirements.

In the study on the current surveillance IT landscape and resulting options [8], five problem statements were identified as barriers to cross-border and cross-sector sharing of information relevant for maritime surveillance. Two problem statements were formulated from the viewpoint of authorities needing information:

- I need some information and I know who has the information ("direct pull").
- I need some information and I do *not* know who has the information ("indirect pull").

Two additional problem statements were described from the viewpoint of authorities having information:

- I have some information that I want or that I need to share and I know who needs this information ("direct push").
- I have some information that I want or that I need to share and I do *not* know who needs this information ("indirect push").

A fifth problem statement was formulated to cover the case of the *undefined unknown*:

- I do not know that I possess information useful to others or I am not aware that I need more information due to partial maritime domain awareness.

These problem statements are reused in the selection criteria to understand each vision's effectiveness in improving maritime surveillance. This is done by describing how the vision contributes to solving the problem statements.

The effectiveness of a vision is also determined by how well it fulfils the requirements for CISE (described in sections 4 and 5). This section will include a summary of the requirements coverage, while the details of the requirements coverage assessment can be found in Annex 4 Requirements coverage in detail.

6.2.2. Efficiency

The efficiency of a vision describes how economic resources can be converted into results. Efficiency focuses on the implementation of the vision and includes the short-term costs and time required to realise the vision. This selection criterion will be based on the results of a costing study [11].

6.2.3. Sustainability

The sustainability of the IT environment is expressed in the environment's ability to present an evolving life-cycle, despite technical barriers, evolving functional requirements and technologies, resource constraints, and changing user preferences. The sustainability of a vision describes the probability of each vision to realise continued, long-term benefits and the long-term costs that are incurred. It focuses on operating CISE in the long-term. This selection criterion will be based on the results of a costing study [11].

CISE Core – Multiple providers of CISE Services at National level (+ EU Initiatives)

The vision at a glance

Description

The core vision is CISE's minimum viable architecture i.e. the minimum collection of building blocks required for CISE to fulfil its most essential requirements.

Public authorities, from the several User Communities, independently offer services to exchange information with other CISE participants. When sharing information with each other, CISE participants not only use common information definitions and structures, but also common technical standards (e.g. messaging protocol). These specifications are used to define CISE-compliant software referred to as a "CISE gateway" which promotes seamless compatibility with existing systems and connectivity with other CISE participants (an optional reference implementation of the gateway can be provided). In this vision CISE participants need to know how each User Community in each Member State is organised to get access to the information they need.

CISE participants are free to choose how they want to move towards CISE given that no governance model is prescribed in this vision.

CISE participants create their own integrated maritime awareness picture by collecting information from multiple sources.

How does this vision improve maritime surveillance?

It improves maritime surveillance by encouraging public authorities, holding information relevant to CISE, to share information with others through commonly defined semantic and technical building blocks (see what interoperability agreements are needed for this Vision below).

What interoperability agreements are needed for this Vision?

At semantic level, interoperability agreements on a common information exchange model, data classification levels, access profiles, catalogue of datasets and information services are needed.

At technical level, an interoperability agreement on a messaging protocol is needed. The messaging protocol is implemented in the CISE gateway.

What changes in this vision, compared to the as-is situation?

To support public authorities wanting to exchange information, several semantic interoperability agreements are commonly defined e.g. an information exchange model. To further facilitate exchanges of classified information, all CISE visions propose commonly agreed data classification levels and a catalogue of datasets.

The CISE CORE also prescribes a messaging protocol implemented in a "CISE gateway". A reference implementation of the gateway can be provided to public authorities to facilitate their moving towards CISE specifications (and becoming a CISE participant by doing so). The use of the CISE gateway

reference implementation is optional. The information received by public authorities is, by default, as it is sent by the information provider, as there are no commonly agreed aggregation and fusion rules of information.

In addition to the above interoperability agreements, common elements are deployed to facilitate real-time collaboration between public authorities. These elements are commonly defined, meaning that they must be used in identical manner by all participants. They do not necessarily need to be deployed centrally.

Common Register of Authorities: a contact directory containing contact details and information about the CISE participants.

Common Collaborative Platform**:** a set of tools that allows virtual collaboration between public authorities. This can include audio and video communication, instant messaging, etc.

Common Monitoring Services: monitors performance and availability of services and can provide statistics. By agreeing on Common Monitoring Services, statistics on provided services are consistent and comparable.

Common Authentication Services: manages all aspects of authentication (i.e. management of certificates). By defining Common Authentication Services, CISE participants are ensured that they rely on the same authentication mechanism, independent of the CISE gateway they are connecting with.

Organisational interoperability

How would authorities (at national, Sea Basin, sectorial and European level) organise themselves to share information relevant for maritime surveillance with one another?

Each authority, in its role as service consumer, needs to understand which services are available through the several authorities in each Member State, User Community and European level initiative. They can use the Common Register of Authorities to retrieve this information. Authorities then need to decide which services to consume based on their specific business needs.

Authorities are free to organise themselves as they see fit. If they choose to collaborate internally and create a single CISE access point at national level (e.g. at the national level), they are free to do so.

What agreements would be needed to enable authorities to share information relevant for maritime surveillance?

This vision requires cross-sectorial information sharing agreements between public authorities belonging to different User Communities, which could be established through interoperability agreements.

How would CISE be operated?

Service desk: Each authority is responsible for setting up its own service desk. A common service desk would be organised to address issues regarding the gateway specifications and its reference implementation.

Application management: Each authority is responsible for its own information sources. The commonly agreed information exchange model, the gateway specifications, the Common Register of Authorities, the Common Authentication Services, the Common Monitoring Services and the Common Collaborative Platform are maintained by a central authority.

IT operations management: Authorities are individually responsible for operating their information systems and their gateways. Each authority, as information source, is responsible for respecting and monitoring the agreements with other authorities with regards to accessing and providing services (if applicable).

Technical management: Authorities are responsible for the technical management of their information systems. Authorities can choose to use the reference implementation of the CISE gateway or to gradually move towards the CISE gateway specifications in their own implementation.

What kind of organizational governance needs to be established?

As authorities collaborate bi-laterally, no organisational governance is prescribed.

Semantic interoperability

How is information made understandable and usable?

Information is shared using a commonly agreed information exchange model, data classification levels and access profiles, catalogue of datasets and information services.

The information exchange model describes how information is structured and what controlled vocabularies and taxonomies are used to describe it; the data classification levels define a common ontology between data types and access rights; and the catalogue of datasets and information services lists all possible CISE services.

How are access rights decided on?

Authorities manage the access rights for the information they own. If they do not own the information, they must respect the applicable licensing.

Technical interoperability

How would authorities be able to share information?

Each public authority must implement a standardised CISE gateway by either using a reference implementation of the gateway or by incrementally moving their existing systems towards the CISE gateway specifications. By doing so, the public authority becomes a CISE participant and can share information with other participants.

Are there specificities for national and Sea Basin authorities?

National authorities are free to decide whether to share information by connecting their systems to a system at national level that gathers information from various sources and then shares it with CISE participants, using CISE' standardised gateway, or by making a direct connection to CISE. An important factor for this decision is the scope of the integrated maritime awareness picture to be offered at Member State level and compliance with existing and planned regulations.

This vision does not foresee the participation of authorities at Sea Basin level.

Are there specificities for EU led initiatives?

EU led initiatives participate at the same level as public authorities.

Agencies and DGs are free to choose how they want to organise their participation in CISE. Depending on the structure of the EU led initiative, whether they want to move towards CISE specifications at central level or Member State level, it is up to them. Agencies and DGs can choose what services they want to offer, as long as they comply with CISE specifications.

Due to the large number of independent CISE participants, a large number of connections can be expected for agencies and DGs to set up and maintain for interested service consumers (e.g. public authorities or other EU led initiatives). Please refer to section 6.3 for preliminary reflections on how

existing EU led initiatives can participate in CISE. It should be noted that the existence of central systems at EU level can accelerate the set-up of CISE services, as their data can be offered through CISE more easily than systems where data is scattered in local systems.

How would authorities be able to add new services?

Authorities adding a new service need to ensure that it is compliant with the CISE specifications (e.g. information exchange model, data classification levels etc.) as defined in the commonly agreed interoperability agreements.

How would authorities discover information relevant for them?

The Common Register of Authorities can be consulted to retrieve information about the authorities that offer services.

How would authorities retrieve information relevant for them?

As the CISE gateway specifications provide standardisation for the information exchange model and the messaging protocol; authorities can connect without additional technical effort to all other authorities implementing the same specifications.

Public authorities are responsible for constructing their own integrated maritime awareness pictures. Similar information may be passed to the requestor several times from different information sources, if the requestor uses similar services from multiple authorities. Therefore, the public authority is responsible for processing the received information as it sees fit e.g. correlating and fusing data.

How are authentication and authorisation handled?

Authorisation is managed by the information providers, respecting any constraints imposed by the information owner. Each CISE participant should implement an information access management system based on the commonly agreed access profiles. Authorities are responsible for classifying their information according to the commonly agreed data classification levels. They do not have to modify their internal classification scheme, however.

The authentication of CISE participants is done through Common Authentication Services in accordance with the CISE access profiles. These services are commonly agreed and implemented by each CISE participant (as part of the gateway specifications) to ensure that authentication is always performed in the same manner. The use of Common Authentication Services is made possible by the standardisation of the messaging protocol. Individual end-users are not authenticated in the Common Authentication Services. Authentication for the use of CISE services will be performed on the level of public authorities. Each authority is responsible for authenticating its end-users. When an authenticated end-user requests or sends information, the authority's assigned CISE access profile will be used in the information exchange. They are responsible for authenticating their end-users. When an authenticated end-user requests or sends information, their assigned CISE access profiles will be used in the information exchange.

Authorisation of CISE information requests and subscriptions is done at the level of the public authority, respecting the CISE access profiles.

The definition of the common services is to be defined, whether these should include specifications, reference implementation and/or services.

How is trust between participants established?

Establishing trust between the different CISE participants system can be enhanced by:

- Building a CISE security policy, specifying minimal security requirements that all CISE users and entities shall respect.
- Applying commonly agreed data classification levels. Correct information classification by all CISE members is a key factor to prevent disclosure of information. There should be a common understanding among all CISE members about what the implications of applying information classification levels are.
- Applying commonly agreed access profiles. Following the same principles as for information classifications, there should be a common understanding of the CISE access level profiles.

How would this vision enable virtual collaboration between authorities?

Authorities can use a Common Collaborative Platform to interact with one another in real-time.

What technical governance is required?

The sustainability of CISE's technical specifications will preferably be done by standardisation bodies.

How adequate is the vision to face technical barriers to interoperability?

Varying capacity of source systems to exchange surveillance and monitoring information	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
Machine-dependent, old architectures make it cumbersome to interconnect with CISE	**Partly**	Partly	Partly	Fully	Fully
Varying data quality across source systems reduces trustworthiness of CISE	**Not**	Not	Not	Fully	Partly
Varying current cross-sectorial integration of Maritime Surveillance within countries creates strong imparities in effort to connect to CISE	**Not**	Not	Not	Partly	Fully
There is a lock-in into modern commercial platform solutions	**Partly**	Partly	Partly	Not	Fully
Lack of interoperability of current systems' landscape	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
There are no common information models (as of yet)	**Fully**	Fully	Fully	Fully	Fully
There are no common technical protocols (as of yet)	**Partly**	Partly	Partly	Fully	Fully
Immature and/or diverging	**Partly**	Partly	Partly	Fully	Fully

definition of metadata between user communities hampers cross-sectorial sharing of information					
Data and metadata will be in different languages	**Fully**	Fully	Fully	Fully	Fully
Existing Node models will need to be integrated	**Fully**	Fully	Fully	Partly	Fully

Rating scale:

- Fully: the barrier is fully or to a very large extent addressed by the Vision
- Partly: the barrier is partly addressed by the Vision
- Not: the Vision is not suited for addressing the barrier.

Architectural building blocks that need to be specified[6]

Central components

Name	Volume
CISE Governance	1
Information Exchange Model	1
Register of services & authorities	1
Common Collaborative Platform	1
Common Monitoring Services	1
Reference Implementation of National Node	0
Reference Implementation of Gateway	1
Cost of connecting EU-level systems	1

Building blocks

Type	Volume
Node	0
Interface	141.2

[6] Definitions of components and building blocks can be found in the Glossary in Annex of this document

SWOT analysis

What are the strengths of this vision?

Possibility to enhance the present sectorial maritime awareness pictures with additional information.

The commonly agreed information exchange model and the gateway specifications increase commonalities in information exchanges.

The standardised connections allow implementing a broadcast notification system.

Security measures to guarantee secure transmission of information can be installed at the level of the gateway. The security measures will be homogeneous across all gateways.

The Vision leaves flexibility to Member States regarding their investments in the Maritime Surveillance domain and the governance structures ruling it.

What are the weaknesses of this vision?

Correlation and fusion rules are not commonly agreed among CISE participants.

Risk of receiving duplicate and contradictory information since there are multiple service providers at Member State level, eventually providing very similar services.

Public administrations need to be able to collect information from multiple sources and process it for a meaningful result.

No governance model is specified.

This Vision is the second most costly.

In terms of sustainability, this Vision will result in a limited improvement of Maritime awareness pictures.

What are the opportunities associated with this vision?

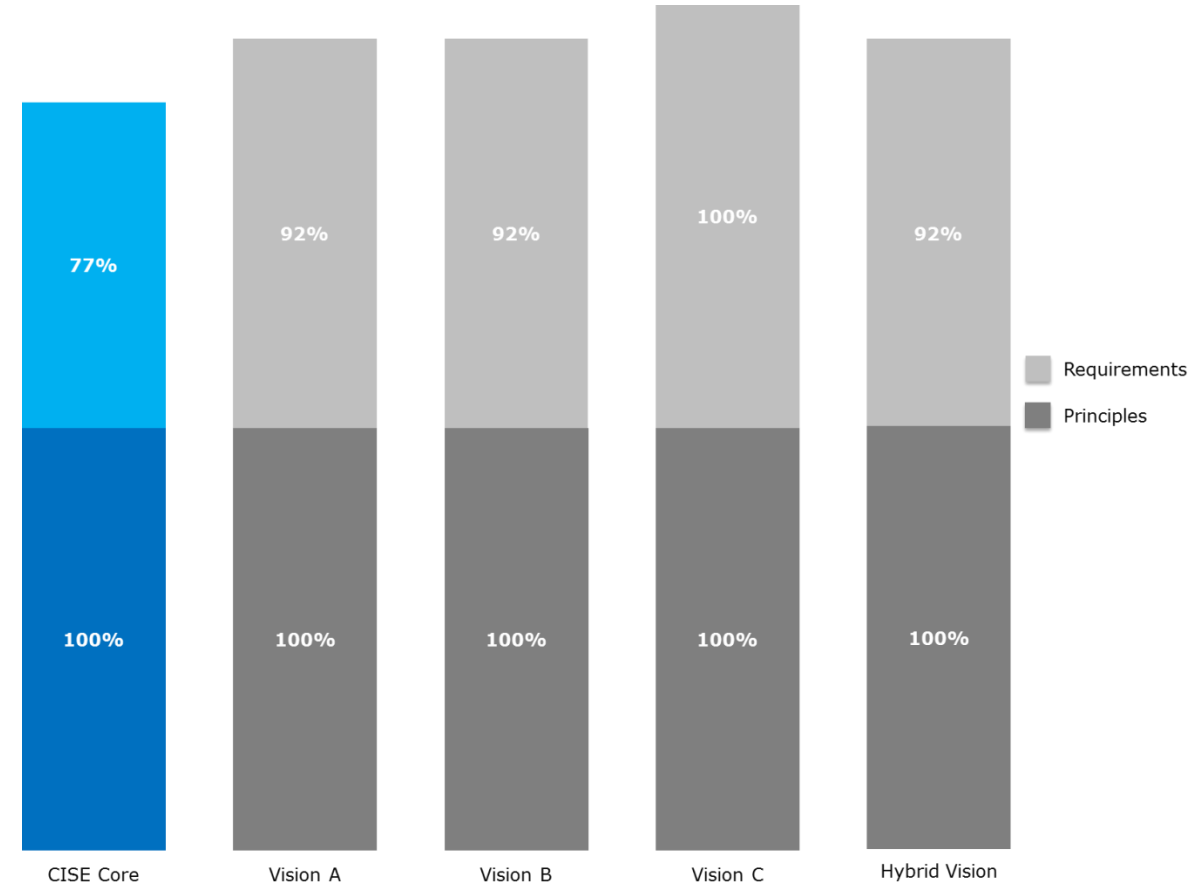
A reference implementation of the gateway can be provided to spur adoption.

What are the threats associated with this vision?

There is little incentive for public authorities to cooperate; they can offer services independently of each other.

Selection criteria

What is this vision's effectiveness in improving maritime awareness?

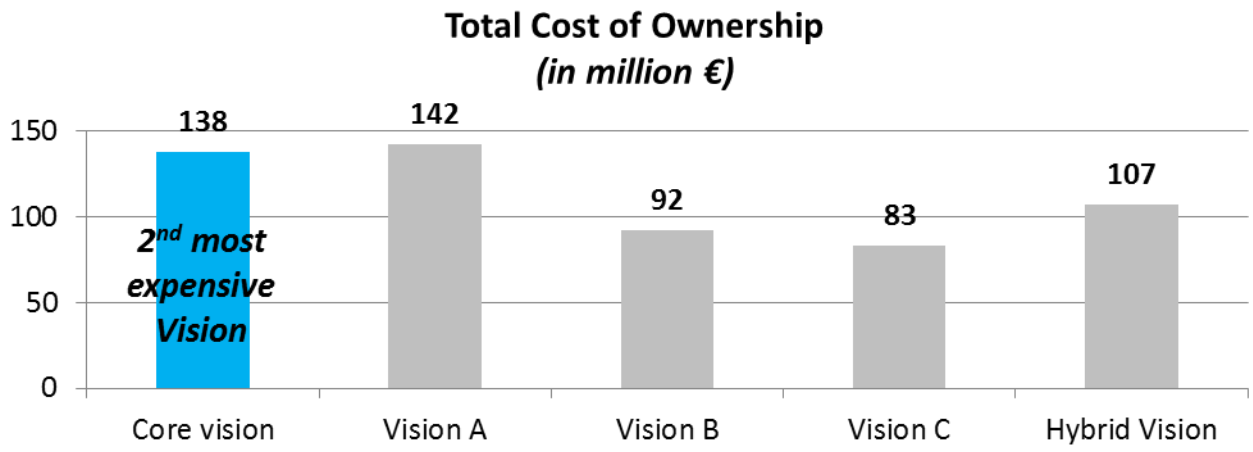


The details of the requirements coverage assessment can be found in Annex 4 .

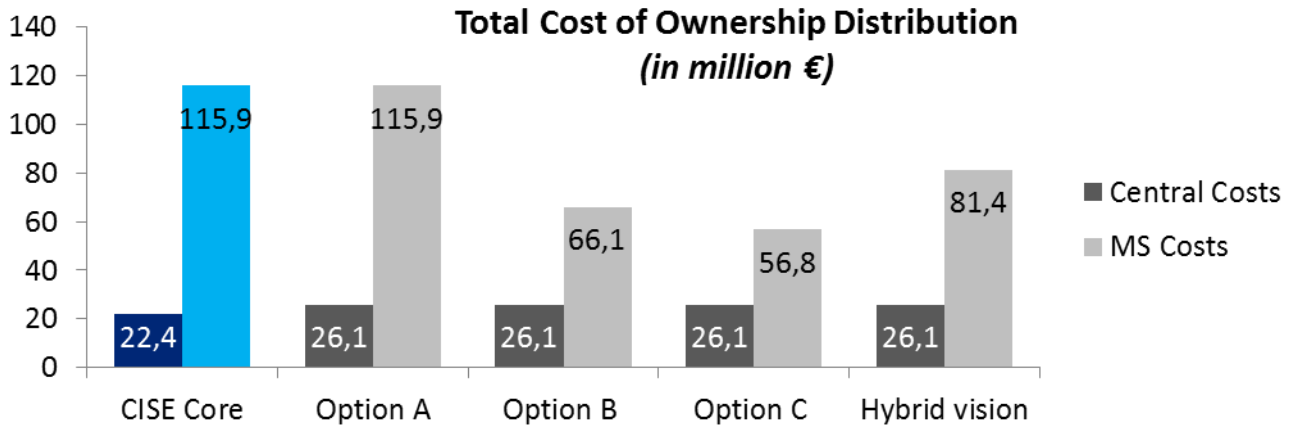
How efficient is this vision in terms of economic resources needed in the short-term?[7]

The CORE Vision is the second most expensive as expressed in Total Cost of Ownership (TOC).

[7] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013



Member States will bear 82% of the initial investment costs (CAPEX) and 73% of the operational costs (OPEX) calculated over 10 years.



How sustainable is this vision? What are the continued long-term benefits?[8]

In terms of sustainability, this Vision will not lead to an improved Maritime awareness picture. The accuracy and usefulness of the awareness picture risk being jeopardized by: heterogeneity in source data quality; the lack of coordination of information content & flows in the exchange; and the lack of common rules for aggregation & analysis.

[8] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013

Vision A – Multiple Providers of CISE Services Coordinated by User Communities (+ EU Initiatives)

The vision at a glance

Description

In this vision, CISE services are offered by public authorities at national and EU level within each User Community. The governance model is centred on User Communities and will be, as much as possible, built upon existing governance bodies.

When sharing information with each other, CISE participants (i.e. public authorities and EU led initiatives) use common information definitions, structures and technical standards. These specifications are used in CISE-compliant software referred to as a "CISE node" (i.e. a gateway which also has the functionality to perform correlation and fusion of information). To facilitate the discovery of services, User Communities set up software referred to as a "CISE service discovery coordinator" which facilitates the discovery of services offered at EU and national level. Because of this, CISE participants no longer need to know which authorities to contact to get access to information. An optional reference implementation of the node and the service discovery coordinator can be provided. EU led initiatives operate their own CISE nodes.

CISE participants create their own integrated maritime awareness picture by collecting information from multiple sources. Due to the governance at User Community level, the maritime awareness pictures created by individual authorities are User Community oriented.

How does this vision improve maritime surveillance?

Improves maritime surveillance by encouraging public authorities holding information relevant to CISE to share information with others through commonly defined semantic, technical and organisational building blocks (see what interoperability agreements are needed for this Vision below).

Public authorities no longer need to be aware of who provides the CISE service; this functionality is now provided by the service discovery coordinators at User Community level.

As in the CISE Core vision, CISE participants must still individually create their own integrated maritime awareness pictures by merging information collected from multiple sources.

What interoperability agreements are needed for this vision?

At semantic level, interoperability agreements on a common information exchange model, data classification levels, access profiles, catalogue of datasets and information services are needed.

For organisational interoperability, an agreement in each User Community is needed to appoint a single public authority in charge of managing their catalogue of services. It is likely that this agreement can rely on existing governance structures within the User Communities.

At technical level, interoperability agreements on a messaging protocol, correlation and fusion rules, and service discovery specifications need to be made. The messaging protocol and correlation and fusion rules are implemented in software referred to as the CISE node. The service discovery specifications are implemented in software referred to as the service discovery coordinator, which

facilitates the consultation of the catalogue of services and their discovery.

What changes in this vision, compared to the other Visions?

This vision relies on User Communities to organise the cross-sector and cross-border information sharing.

Unlike the CISE core vision; this vision facilitates information sharing through the use of a standardised CISE node, which is capable of information fusion and correlation. The service discovery coordinators at the User Community level facilitate the dynamic identification of service providers.

Organisational interoperability

How would authorities (at national, Sea Basin, sectorial and European level) organise themselves to share information relevant for maritime surveillance with one another?

Each User Community appoints a single public authority that is responsible for managing the User Community's catalogue of services, composed of the services offered by all public authorities within the User Community in the several Member States. Management of the service catalogue includes e.g. ensuring the overall coherence of the offered services, ensuring there are no duplicate services, etc. Public authorities wanting to offer services contact this single public authority to register their services.

What agreements would be needed to enable authorities to share information relevant for maritime surveillance?

This vision may require bilateral cross-sectorial information sharing agreements between public authorities belonging to different User Communities or cross-User Community agreements.

How would CISE be operated?

Service desk: The service desk is to be set up at public authority level in conjunction with its node. User Community level help desks are needed for the service discovery coordinators. A central help desk supports the implementations of the node specifications by public authorities and EU led initiatives.

Application management: Application management of the end-user system that manages connections to the authority node is dealt with by each individual authority. The application management of each service discovery coordinator is handled at User Community level. The commonly agreed data classification levels, catalogue of datasets, information exchange model, the node and service discovery coordinator specifications, the Collaborative Platform, the Common Monitoring Services, the Common Authentication Services and Common Register of Authorities must be maintained by a central authority.

IT operations management: Authorities as information sources are responsible for respecting the CISE specifications relating to accessing and providing services. User Communities are responsible for ensuring that the service discovery coordinator fulfils the CISE specifications. It is up to each authority to set up Monitoring Services used to monitor performance and to collect statistics from their node. The User Community authority may also play a role such as consolidating the information received from the several CISE participants.

Technical management: Authorities and EU led initiatives are responsible for the technical management of their information systems. They can choose to use the reference node implementation or to gradually move towards the CISE specifications in their own implementation. In a similar fashion, User Communities can choose to use the reference implementation of the service discovery coordinator or to gradually move towards the CISE specifications in their own implementation. The use of the CISE node and coordinator reference implementations is optional.

What kind of organizational governance needs to be established?

User Communities must establish governance around the single public authority in charge of the service catalogue. This governance structure will, as much as possible, leverage existing governance bodies.

Semantic interoperability

How is information made understandable and usable?

Information is shared using a commonly agreed information exchange model, data classification levels and access profiles, catalogue of datasets and information services.

The information exchange model describes how information is structured and what controlled vocabularies and taxonomies are used to describe it; the data classification levels define a common ontology between data types and access rights; and the catalogue of datasets lists all possible CISE services.

How are access rights decided on?

Authorities manage the access rights for the information they own. If they do not own the information, they must respect the applicable licensing.

Technical interoperability

How would authorities be able to share information?

Each public authority must implement CISE node specification by either using a reference implementation of the node or by incrementally moving their existing systems towards the CISE node specifications. By doing so, the public authority becomes a CISE participant and can consult the service discovery coordinators and exchange information with other CISE.

The single public authority in each User Community in charge of managing the service catalogue is responsible for implementing a standardised CISE service discovery coordinator by either using a reference implementation of the service discovery coordinator or by incrementally moving their existing systems towards the CISE service discovery coordinator specifications. The service discovery coordinator enables automated discovery of the services in the service catalogue of EU led initiatives or authorities at Member State level.

Broadcasting of information can be facilitated by the service discovery coordinators by expanding their functionality to holders of subscriptions to “publish/ subscribe” services.

Are there specificities for national and Sea Basin authorities?

National authorities are free to decide whether to share information by connecting their systems to a system at national level that gathers information from various sources and then shares it with CISE participants, using CISE’ standardised gateway, or by making a direct connection to CISE. An important factor for this decision is the scope of the integrated maritime awareness picture to be offered at Member State level and compliance with existing and planned regulations. Unlike the CISE Core, these decisions should be coordinated by the User Community authority.

This vision does not foresee the participation of authorities at Sea Basin level.

Are there specificities for EU led initiatives?

EU agencies and European Commission DGs hosting an EU level initiative will be impacted in the same manner as in the CISE Core architecture. The only difference is that there is a single authority at User Community level that manages a service discovery coordinator with a catalogue of services composed of all the services that authorities within a User Community provide at Member State or EU level.

Similarly to the CISE Core architecture, agencies and DGs are also free to choose how they want to organise their participation in CISE - whether they want to move towards CISE node specifications at central level or at Member State level - is up to them.

Please refer to section 6.3 for preliminary reflections on how existing EU led initiatives are impacted by CISE. It should be noted that the existence of central systems at EU level can accelerate the setup of CISE services, as their data can be offered through CISE more easily than systems where data is scattered in local systems.

How would authorities be able to add new services?

Public authorities wanting to offer a new service must contact the single public authority in their User Community that manages the services catalogue to register their service. A public authority offering a service must use the commonly agreed information exchange model and must be compliant with the CISE node specifications.

How would authorities discover information relevant for them?

To discover information, a public authority consults the User Community service discovery coordinators. By consulting the coordinators, public authorities learn what services are offered and what public authorities offer them.

The service discovery is an automated process. Public authorities use their node to connect to service discover coordinators to find out the location of the service provider so that they can contact it. The service discovery coordinator returns this location to the requesting node, which can then establish a connection to the node of the service provider. Due to the automated process of service discovery, CISE participants no longer need to know other User Communities' internal structures in order to exchange information.

How would authorities retrieve information relevant for them?

Authorities wishing to consume information services use their node to consult a User Community service discovery coordinator to learn where those services are offered. The service discovery coordinator only provides the location of those services so that a connection between the node of the service consumer and the service provider can be established.

Similar information may be passed to the requestor several times from different information sources if similar services are provided by multiple authorities. This issue can be prevented at User Community level by applying certain rules to the discovery of services in the coordinator to restrict the number of service providers and to ensure overall coherence between the services offered. The issue might still persist in cross-sector information exchanges, if similar information is requested and provided by public authorities in different User Communities. Therefore, the public authority is responsible for processing

the received information as it sees fit e.g. correlating and fusing data. Public authorities are responsible for constructing an integrated maritime awareness picture.

How are authentication and authorisation handled?

Authorisation is managed by the information providers, respecting any constraints imposed by the information owner. Each CISE participant should implement an information access management system based on the commonly agreed access profiles. Authorities are responsible for classifying their information according to the commonly agreed information classification scheme. They do not have to modify their internal classification scheme however.

The authentication of CISE participants is done through Common Authentication Services in accordance with the CISE access profiles. These services are commonly agreed and implemented by each CISE participant (as part of the node specifications) to ensure that authentication is always performed in the same manner. The use of Common Authentication Services is made possible by the standardisation of the messaging protocol. Authentication of CISE information requests and subscriptions is done at the level of the public authority. Individual end-users are not authenticated in the Common Authentication Services.

Authorities are responsible for assigning one or more CISE access profiles to their end-users. They are responsible for authenticating their end-users. When an authenticated end-user requests or sends information, their assigned CISE access profiles will be used in the information exchange.

The definition of the common services are to be defined, whether these should include specifications, reference implementation and/or services.

How is trust between participants established?

Establishing trust between the different CISE participants system can be enhanced by:

- Building a CISE security policy, specifying minimal security requirements that all CISE users and entities shall respect.
- Applying commonly agreed classification levels. Correct information classification by all CISE members is a key factor to prevent disclosure of information. There should be a common understanding among all CISE members about what the implications of applying information classification levels are.
- Applying commonly agreed access profiles. Following the same principles as for information classifications, there should be a common understanding of the CISE access level profiles.

How would this vision enable virtual collaboration between authorities?

Authorities can use a Common Collaborative Platform to interact with one another.

What technical governance is required?

The sustainability of CISE's technical specifications will preferably be done by standardisation bodies.

How adequate is the vision to face technical barriers to interoperability?

Varying capacity of source systems to exchange surveillance and monitoring information	Adequateness of Vision				
	Core	**A**	**B**	**C**	**Hybrid**
Machine-dependent, old architectures make it cumbersome to interconnect with CISE	Partly	**Partly**	Partly	Fully	Fully
Varying data quality across source systems reduces trustworthiness of CISE	Not	**Not**	Not	Fully	Partly
Varying current cross-sectorial integration of Maritime Surveillance within countries creates strong imparities in effort to connect to CISE	Not	**Not**	Not	Partly	Fully
There is a lock-in into modern commercial platform solutions	Partly	**Partly**	Partly	Not	Fully
Lack of interoperability of current systems' landscape	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
There are no common information models (as of yet)	Fully	**Fully**	Fully	Fully	Fully
There are no common technical protocols (as of yet)	Partly	**Partly**	Partly	Fully	Fully
Immature and/or diverging definition of metadata between user communities hampers cross-sectorial sharing of information	Partly	**Partly**	Partly	Fully	Fully
Data and metadata will be in different languages	Fully	**Fully**	Fully	Fully	Fully
Existing Node models will need to be integrated	Fully	**Fully**	Fully	Partly	Fully

Rating scale:

- Fully: the barrier is fully or to a very large extent addressed by the Vision
- Partly: the barrier is partly addressed by the Vision
- Not: the Vision is not suited for addressing the barrier.

Architectural building blocks that need to be specified[9]

Central components

Name	Volume
CISE Governance	1
Information Exchange Model	1
Register of services & authorities	1
Common Collaborative Platform	1
Common Monitoring Services	1
Reference Implementation of National Node	1
Reference Implementation of Gateway	0
Cost of connecting EU-level systems	1

Building blocks

Type	Volume
Node	0
Interface	141.2

[9] Definitions of components and building blocks can be found in the Glossary in Annex of this document.

SWOT analysis

What are the strengths of this vision?

Possibility to enhance the present sectorial maritime awareness pictures with additional information.

The commonly agreed information exchange model and the node specifications increase commonalities in information exchanges.

Common rules for correlation and fusion of information are agreed enabling the creation of harmonised integrated maritime awareness pictures.

Authorities can more easily discover services through the service discovery coordinators of each User Community; they no longer need to know upfront where the service they need is offered.

User Communities decide what services should be in their service catalogue.

What are the weaknesses of this vision?

Risk of receiving duplicate and contradictory information since there are multiple service providers at Member State level, eventually providing very similar services.

This vision may require bilateral cross-sectorial information sharing agreements between public authorities belonging to different User Communities or cross-User Community agreements.

This Vision is the most costly of all choices; the main cost driver of this Vision is the lack of centralisation meaning that neither investments nor operating cost and procedures are streamlined.

In terms of sustainability, this Vision bears a significant risk induced by the lack of an overall "national" Maritime awareness picture.

What are the opportunities associated with this vision?

A CISE reference implementation of the node can be provided to spur adoption.

The CISE service discovery coordinator can facilitate the discovery of all information services relevant for maritime surveillance.

A fall-back mode based on interconnected public authorities could be considered in case of major attacks or unavailability of the User Community coordinator.

Possibility to reduce duplication and overlap of data and services.

What are the threats associated with this vision?

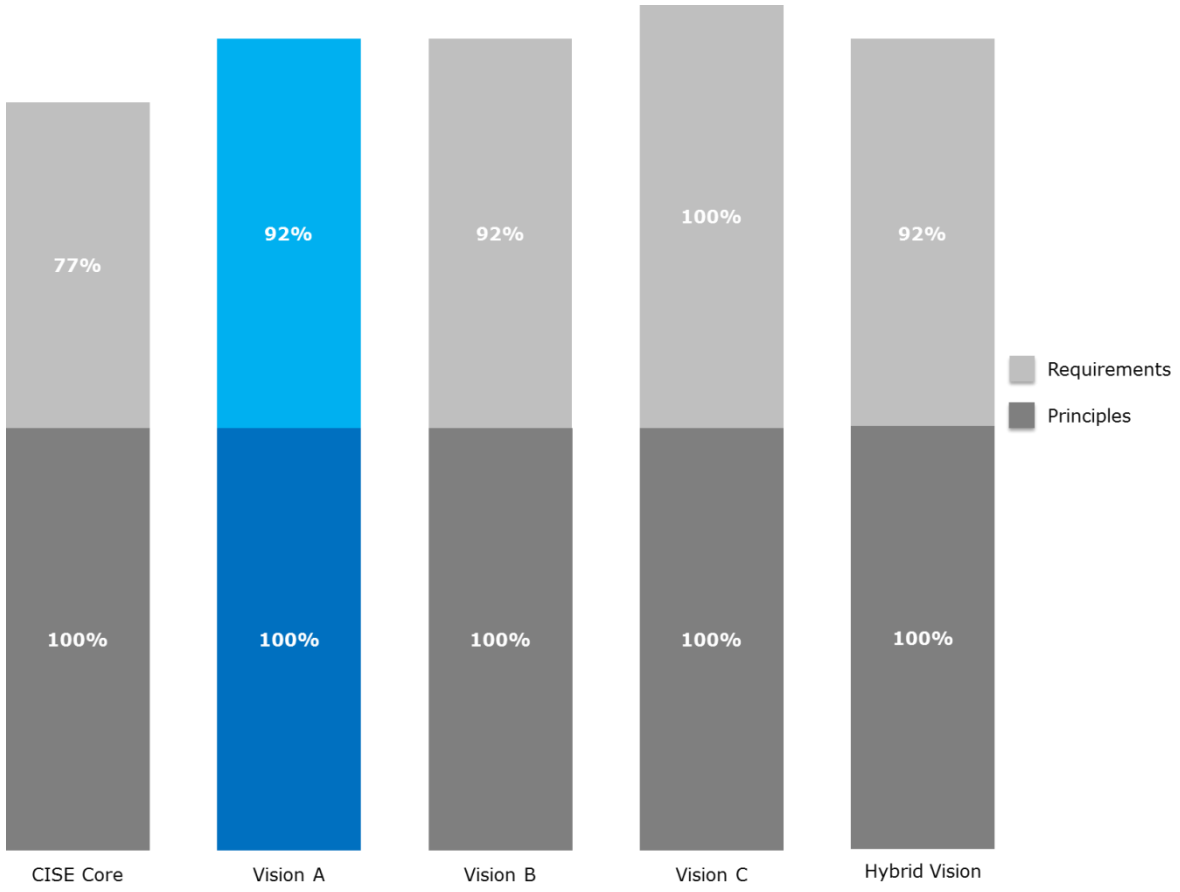
There is little incentive for public authorities to cooperate beyond their User Community; as each one of them offers services independently of each other.

User Communities might need to establish a new authority to manage the service catalogue and to operate the service discovery coordinator.

A service discovery coordinator at User Community level can be perceived as a single point of failure; without it, the services offered in the User Community catalogue are no longer discoverable. This can however be dealt at the physical level, where the "single node" can/ be converted into "multiple nodes".

Selection criteria

What is this vision's effectiveness in improving maritime awareness?

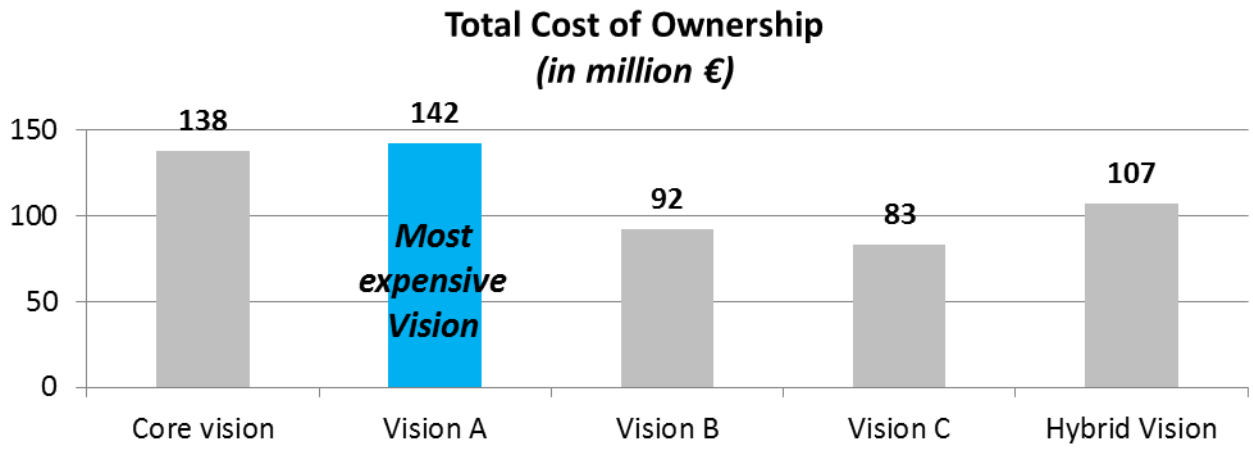


The details of the requirements coverage assessment can be found in Annex 4 .

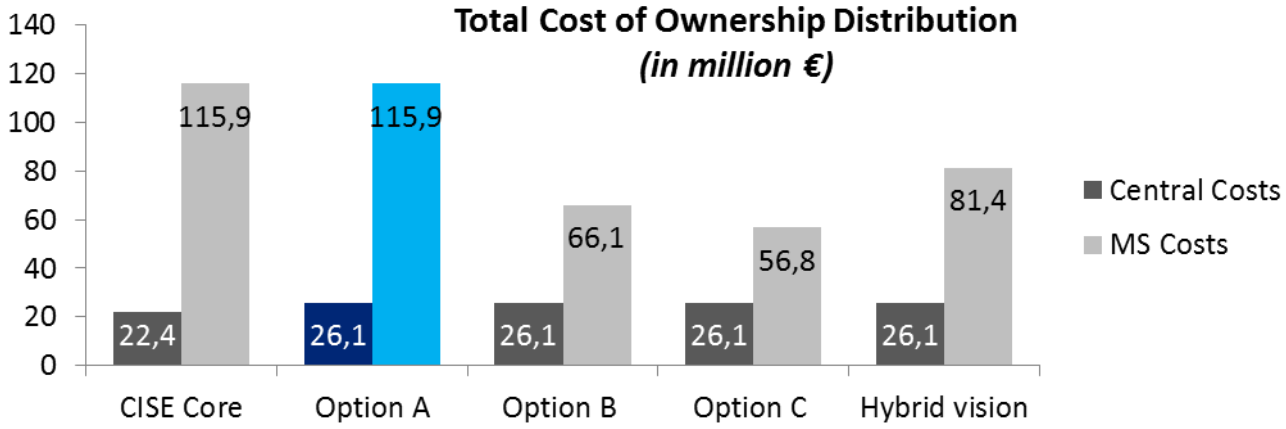
How efficient is this vision in terms of economic resources needed in the short-term?[10]

Vision A is the most expensive as expressed in Total Cost of Ownership (TOC).

[10] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013



Member States will bear 80% of the initial investment costs (CAPEX) and 72% of the operational costs (OPEX) calculated over 10 years.



How sustainable is this vision? What are the continued long-term benefits?[11]

In terms of sustainability, this Vision bears a significant risk induced by the lack of an overall "national" Maritime awareness picture. This is due to: heterogeneity in quality of source data, the lack of coordination of information/ content flows and the lack of common rules for aggregation & analysis.

[11] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013

Vision B – Multiple Providers of CISE Services Coordinated by Member States (+ EU Initiatives)

The vision at a glance

Description

Unlike the previous visions, each Member State nominates an authority to manage its catalogue of services, which is composed of the set of services offered by authorities within its borders. To facilitate the discovery of services, Member States set up software referred to as a "CISE service discovery coordinator" (unlike Vision A, the service catalogues are managed by each Member State instead of User Communities). A similar coordinator is set up at EU level to facilitate the discovery of services offered by EU led initiatives. CISE participants consult the coordinators to know where the service they want to use is offered. CISE participants do not need to know which authorities to contact to get access to information.

Public authorities and EU led initiatives, from the several User Communities, offer a set of services to other CISE participants. When sharing information with each other CISE participants use common information definitions, structures and technical standards. These specifications are used in CISE-compliant software referred to as a "CISE node" (similar as in Vision A). Reference implementations of the node and the service discovery coordinator can be provided for optional use.

CISE participants create their own integrated maritime awareness pictures by collecting information from multiple sources. Due to the governance at Member State level, the maritime awareness pictures created by individual authorities are Member State oriented.

How does this vision improve maritime surveillance?

Improves maritime surveillance by encouraging public authorities holding information relevant to CISE to share information using a commonly agreed information exchange model and to offer services using a commonly agreed messaging protocol. As in Vision A, public authorities do not need to be aware of where to get information; this functionality is provided by service discovery coordinators at national and at EU level. Also as in Vision A, CISE participants must individually create their own integrated maritime awareness pictures by merging information collected from multiple sources.

What interoperability agreements are needed for this vision?

At semantic level, interoperability agreements on a common information exchange model, data classification levels, access profiles, catalogue of datasets and information services are needed.

For organisational interoperability, an agreement in each Member State is needed to appoint a single public authority in charge of managing their catalogue of services. It is likely that this is agreement can rely on existing governance structures within the Member State.

At technical level, interoperability agreements on a messaging protocol, correlation and fusion rules, and service discovery specifications need to be made. The messaging protocol and correlation and fusion rules are implemented in software referred to as the CISE node. The service discovery specifications are implemented in software referred to as the service discovery coordinator, which

facilitates the consultation of the catalogue of services.

What changes in this vision, compared to vision A?

The discovery of services is made through service discovery coordinators at Member State level instead of at User Community level. This happens because of a change at organisational level, instead of User Community centric, this vision relies on governance at Member State level and, in particular, the creation of a single authority managing the CISE services offered by a Member State. In this vision, multiple service providers may coexist.

Organisational interoperability

How would authorities (at national, Sea Basin, sectorial and European level) organise themselves to share information relevant for maritime surveillance with one another?

Each Member State appoints a single public authority that is responsible for managing a national catalogue of services, composed of the services offered by all public authorities within its borders. Management of the service catalogue includes e.g. ensuring the overall coherence of the offered services, ensuring there are no duplicate services, etc. Public authorities wanting to offer services contact this single public authority to register their services.

What agreements would be needed to enable authorities to share information relevant for maritime surveillance?

The interoperability agreements should enable the sharing of information among different CISE participants.

How would CISE be operated?

Service desk: The service desk is to be set up on public authority level in conjunction with its node. Member State level help desks are needed for the national service discovery coordinators. A central help desk supports the implementations of the node specifications by public authorities and EU led initiatives.

Application management: Application management of the end-user system that manages connections to the authority node is dealt with at each individual authority. The application management of each national service discovery coordinator is handled on Member State level. The commonly agreed information exchange model, the node and service discovery coordinator specifications, the Common Register of Authorities, the Common Authentication Services and the Common Collaborative Platform are maintained by a central authority.

IT operations management: Authorities as information sources are responsible for respecting the interoperability agreements for accessing and providing services. Member States are responsible for ensuring that the national coordinator fulfils the interoperability agreement for accessing and providing service information. It is up to each authority to set up Monitoring Services used to monitor performance and to collect statistics from their node.

Technical management: Authorities and EU led initiatives are responsible for the technical management of their information systems. They can choose to use the reference implementation of the node or to gradually move towards the CISE specifications in their own implementation. In a similar fashion, Member States and EU led initiatives can choose to use the reference implementation of the service discovery coordinator or to gradually move towards the CISE specifications in their own implementation. The use of the CISE node and coordinator reference implementations is optional.

What kind of organizational governance needs to be established?

Member States must establish governance around the single public authority in charge of their service catalogue. EU level initiatives need to establish a governance structure to manage their services.

Semantic interoperability

How is information made understandable and usable?

Information is shared using a commonly agreed information exchange model, data classification levels and access profiles, catalogue of datasets and information services.

The information exchange model describes how information is structured and what controlled vocabularies and taxonomies are used to describe it; the data classification levels define a common ontology between data types and access rights; and the catalogue of datasets lists all possible CISE services.

How are access rights decided on?

Authorities manage the access rights for the information they own. If they do not own the information, they must respect the applicable licensing.

Technical interoperability

How would authorities be able to share information?

Each public authority must implement a standardised CISE node by either using a reference implementation of the node or by incrementally moving their existing systems towards the CISE node specifications. By doing so, the public authority becomes a node in CISE and can establish standardised connections to national service discovery coordinators (i.e. to discover services offered in Member States) and to other CISE nodes (to exchange information with other public authorities). A service discovery coordinator is also available to facilitate the discovery of the services offered by the EU led initiatives.

The single public authority in charge of managing the service catalogue is responsible for implementing a standardised CISE service discovery coordinator by either using a reference implementation of the service discovery coordinator or by incrementally moving their existing systems towards the CISE service discovery coordinator specifications. The service discovery coordinator enables automated discovery of the services in the service catalogue by public authorities.

Broadcasting of information can be facilitated by the service discovery coordinators by expanding their functionality to holders of subscriptions to “publish/ subscribe” services.

Are there specificities for national and Sea Basin authorities?

National authorities are free to decide whether to share information by connecting their systems to a system at national level that gathers information from various sources and then shares it with CISE participants, using CISE’ standardised gateway, or by making a direct connection to CISE. An important factor for this decision is the scope of the integrated maritime awareness picture to be offered at Member State level and compliance with existing and planned regulations. Unlike Vision A, these decisions should be coordinated by Member State authorities.

This vision does not foresee the participation of authorities at Sea Basin level.

Are there specificities for EU led initiatives?

EU agencies or European Commission DGs are affected in the same manner as in vision A. The only difference is that there is a single authority at EU level that manages a service discovery coordinator with a catalogue of services composed of all the services that EU led initiatives provide.

Please refer to section 6.3 for preliminary reflections on how existing EU led initiatives are impacted by CISE. It should be noted that the existence of central systems at EU level can accelerate the setup of CISE services, as their data can be offered through CISE more easily than systems where data is scattered in local systems.

How would authorities be able to add new services?

Public authorities wanting to offer a new service must contact the single public authority in their Member State that manages the services catalogue to register their service. A public authority offering a service must use the commonly agreed information exchange model and must be compliant with the CISE node specifications.

How would authorities discover information relevant for them?

To discover information, a public authority consults the Member State and EU level service discovery coordinators. By consulting the coordinators, public authorities learn what services are offered and what public authorities offer them.

Service discovery is an automated process. Public authorities use their node to connect to a coordinator to find out the location of the service provider so that they can contact it. The coordinator returns this location to the requesting node which can then establish a connection to the node of the service provider. Due to the automated process of service discovery, CISE participants no longer need to know other User Communities and Member States' internal structures in order to exchange information.

How would authorities retrieve information relevant for them?

Authorities wishing to consume information services use their node to consult the Member State and EU level service discovery coordinators to learn where those services are offered. The service discovery coordinator only provides the location of those services so that a connection between the node of the service consumer and the service provider can be established.

Similar information may be passed to the requestor several times from different information sources if similar services are provided by multiple authorities. This issue can be prevented at national level by applying certain rules to the discovery of services in the coordinator to restrict the number of service providers and to ensure overall coherence between the services offered. The issue might still persist in cross-border information exchanges, if similar information is requested and provided by public authorities in different Member States. Public authorities are responsible for constructing an integrated maritime awareness picture.

How are authentication and authorisation handled?

Authorisation is managed by the information providers, respecting any constraints imposed by the information owner. Each CISE participant should implement an information access management system based on the commonly agreed access profiles. Authorities are responsible for classifying their

information according to the commonly agreed information classification scheme. They do not have to modify their internal classification scheme however.

The authentication of CISE participants is done through Common Authentication Services in accordance with the CISE access profiles. These services are commonly agreed and implemented by each CISE participant (as part of the node specifications) to ensure that authentication is always performed in the same manner. The use of Common Authentication Services is made possible by the standardisation of the messaging protocol. Authentication of CISE information requests and subscriptions is done at the level of the public authority. Individual end-users are not authenticated in the Common Authentication Services.

Authorities are responsible for assigning one or more CISE access profiles to their end-users. They are responsible for authenticating their end-users. When an authenticated end-user requests or sends information, their assigned CISE access profiles will be used in the information exchange.

The definition of the common services are to be defined, whether these should include specifications, reference implementation and/or services.

How is trust between participants established?

Establishing trust between the different CISE participants system can be enhanced by:

- Building a CISE security policy, specifying minimal security requirements that all CISE users and entities shall respect.
- Applying commonly agreed classification levels. Correct information classification by all CISE members is a key factor to prevent disclosure of information. There should be a common understanding among all CISE members of what are the implications of applying information classification levels.
- Applying commonly agreed access profiles. Following the same principles as for information classifications, there should be a common understanding of the CISE access level profiles.

How would this vision enable virtual collaboration between authorities?

Authorities can use a Common Collaborative Platform to interact with one another.

What technical governance is required?

The sustainability of CISE's technical specifications will preferably be done by standardisation bodies.

How adequate is the vision to face technical barriers to interoperability?

Varying capacity of source systems to exchange surveillance and monitoring information	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
Machine-dependent, old architectures make it cumbersome to interconnect with CISE	Partly	Partly	**Partly**	Fully	Fully
Varying data quality across source systems reduces trustworthiness of CISE	Not	Not	**Not**	Fully	Partly
Varying current cross-sectorial integration of Maritime Surveillance within countries creates strong imparities in effort to connect to CISE	Not	Not	**Not**	Partly	Fully
There is a lock-in into modern commercial platform solutions	Partly	Partly	**Partly**	Not	Fully
Lack of interoperability of current systems' landscape	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
There are no common information models (as of yet)	Fully	Fully	**Fully**	Fully	Fully
There are no common technical protocols (as of yet)	Partly	Partly	**Partly**	Fully	Fully
Immature and/or diverging definition of metadata between user communities hampers cross-sectorial sharing of information	Partly	Partly	**Partly**	Fully	Fully
Data and metadata will be in different languages	Fully	Fully	**Fully**	Fully	Fully
Existing Node models will need to be integrated	Fully	Fully	**Fully**	Partly	Fully

Rating scale:

- Fully: the barrier is fully or to a very large extent addressed by the Vision
- Partly: the barrier is partly addressed by the Vision
- Not: the Vision is not suited for addressing the barrier.

Architectural building blocks that need to be specified[12]

Central components

Name	Volume
CISE Governance	1
Information Exchange Model	1
Register of services & authorities	1
Common Collaborative Platform	1
Common Monitoring Services	1
Reference Implementation of National Node	1
Reference Implementation of Gateway	0
Cost of connecting EU-level systems	1

Building blocks

Type	Volume
Node	6
Interface	63.2

SWOT analysis

What are the strengths of this vision?

Possibility to enhance the present sectorial maritime awareness pictures with additional information

The commonly agreed information exchange model and the node specifications increase commonalities in information exchanges.

Common rules for correlation and fusion of information are agreed enabling the creation of harmonised integrated maritime awareness pictures.

Authorities can more easily discover services through the national discovery coordinators; they no longer need to know upfront where the service they need is offered.

Member States decide what services should be in their service catalogue.

What are the weaknesses of this vision?

Risk of receiving duplicate and contradictory information since there are multiple service providers at Member State level, eventually providing very similar services.

CISE participants must be able to create their own integrated maritime awareness picture. They need to be able to collect information from multiple sources and process it for a meaningful result.

In terms of sustainability, this Vision bears a significant risk induced by the lack of an overall “national” Maritime awareness picture.

[12] Definitions of components and building blocks can be found in the Glossary in Annex of this document.

It is expected that Vision B increases the extent of cross-sectorial collaboration within Member States

Vision B leaves room to Member States as to how to implement the interconnection with CISE in respect of their current governance structures and on-going & planned financial investment cycles. Member States can build a single national node or many.

What are the opportunities associated with this vision?

A reference implementation of the node can be provided to spur adoption.

The CISE service discovery coordinator can facilitate the discovery of all information services relevant for maritime surveillance.

A fall-back mode based on interconnected public authorities could be considered in case of major attacks or unavailability of the national coordinator.

Possibility to reduce duplication and overlap of data and services.

What are the threats associated with this vision?

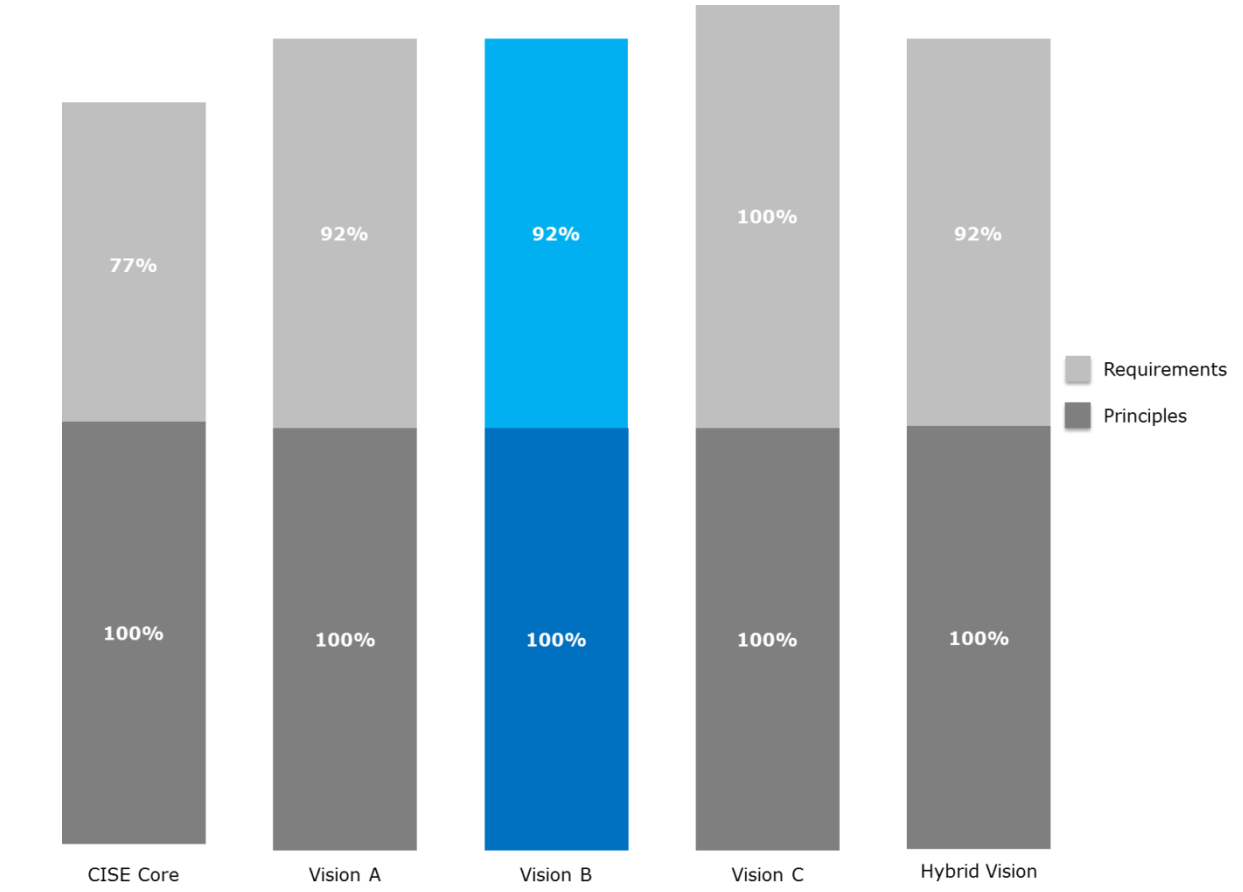
There is little incentive for public authorities to cooperate; they can offer services independently of each other.

Member States might need to establish a new national authority to manage the service catalogue and to operate the coordinator.

A coordinator at national level can be perceived as a single point of failure; without it, the services offered in the national service catalogue are no longer discoverable. This can however be dealt at the physical level, where the “single node” can/ be converted into “multiple nodes”.

Selection criteria

What is this vision's effectiveness in improving maritime awareness?

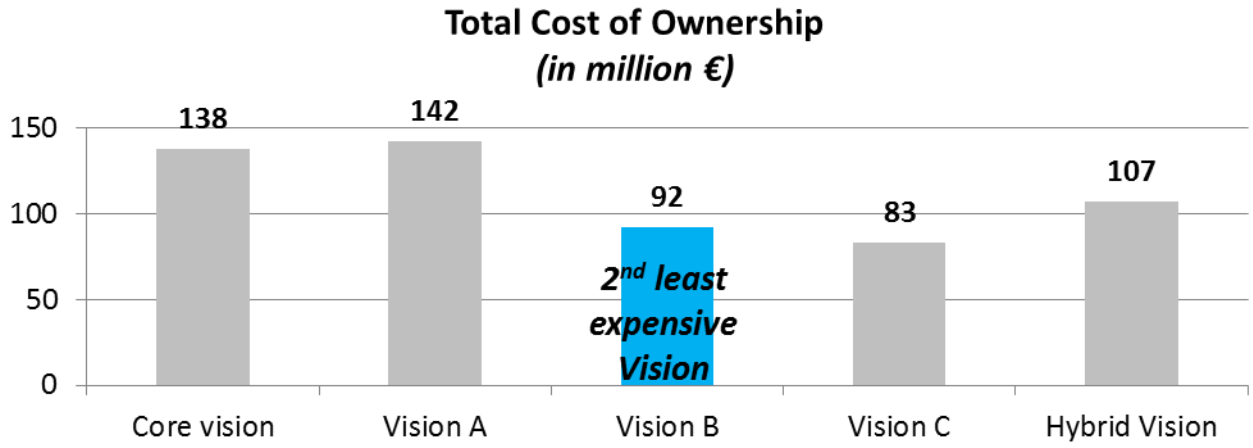


The details of the requirements coverage assessment can be found in Annex 4 .

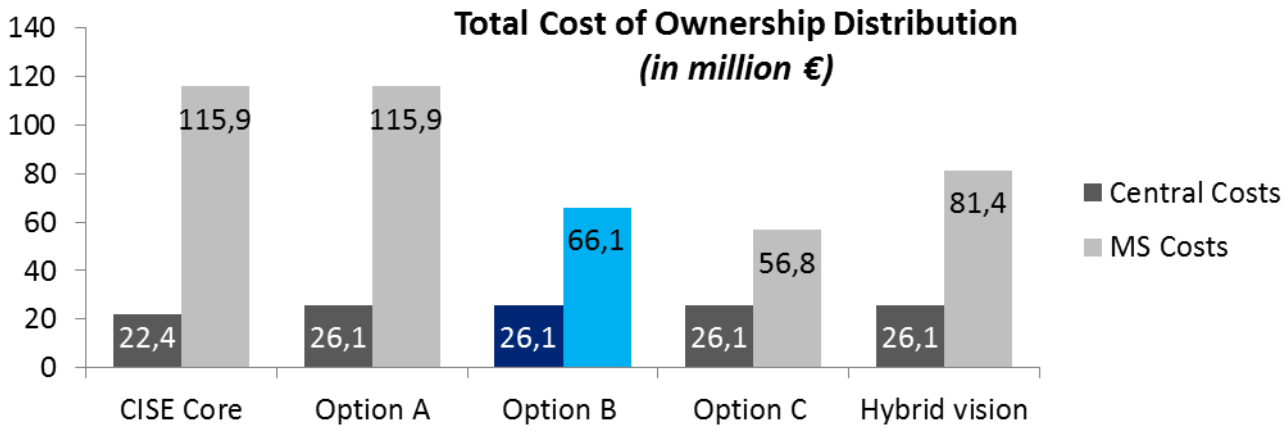
How efficient is this vision in terms of economic resources needed in the short-term?[13]

Vision B is the second least expensive as expressed in Total Cost of Ownership (TOC).

[13] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013



Member States will bear 69% of the initial investment costs (CAPEX) and 60% of the operational costs (OPEX) calculated over 10 years.



How sustainable is this vision? What are the continued long-term benefits?[14]

In terms of sustainability, this Vision bears a significant risk induced by the lack of an overall "national" Maritime awareness picture. This is due to: heterogeneity in quality of source data, the lack of coordination of information/ content flows and the lack of common rules for aggregation & analysis.

[14] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013

Vision C – Single National Providers of CISE Services (+ EU Initiatives)

The vision at a glance

Description

Unlike the previous visions, CISE services are provided by a single Member State authority and EU led initiatives. At Member State level, the single service provider redistributes information collected from the several public authorities within its borders. Because of this, a single integrated maritime awareness picture can be offered per Member State.

As in vision B, when sharing information with each other, CISE participants use common information definitions, structures and technical standards. These specifications are used in CISE-compliant software referred to as a "CISE node" (unlike the previous visions, in this vision, each Member State has a single node). EU led initiatives operate their own CISE nodes.

CISE participants use the services offered by the CISE nodes operated by Member States and EU led initiatives. A "CISE EU service discovery coordinator" is set up at EU level to facilitate the discovery of services offered by EU led initiatives. An optional reference implementation of the node and the service discovery coordinator can be provided.

The main difference between visions B and C is that C has a single national node at Member State level. In both of them, each Member State is required to nominate a single authority to manage its services.

Vision C has a variant, whereby Sea Basin Authorities are set up to operate CISE nodes at sea basin level. In this case, a single integrated maritime awareness picture can be provided for each sea basin. Their services may also be discovered through the service discovery coordinator. This vision is only a variant because the political or operational necessity of sea basin level governance has not been proved so far.

How does this vision improve maritime surveillance?

Improves maritime surveillance by encouraging information systems holding information relevant for it to share information using a commonly agreed information exchange model and a single national node. Through the national node, Member States share cross-sector consolidated information. Public authorities no longer need to be aware of where to get information; this functionality is now provided for by the national CISE node.

In this vision, the national nodes are able to offer a common integrated maritime awareness picture as a service. Public authorities can still individually create their own integrated maritime awareness picture using the services from their national node.

What interoperability agreements are needed for this vision?

At semantic level, interoperability agreements on a common information exchange model, data classification levels, access profiles, catalogue of datasets and information services are needed.

For organisational interoperability, an agreement in each Member State is needed to appoint a single public authority in charge of managing their catalogue of services and the single provider of CISE

providers. These decisions should build upon existing governance structures within the Member State.

At technical level, interoperability agreements on a messaging protocol, correlation and fusion rules, and service discovery specifications need to be made. The messaging protocol and correlation and fusion rules are implemented in software referred to as the CISE node. The service discovery specifications are implemented in software referred to as the service discovery coordinator, which facilitates the consultation of the catalogue of services.

What changes in this vision, compared to vision B?

In this Vision, services are offered through a single national node using information collected from the public authorities within the same Member State and from other CISE participants (i.e. nodes of other Member States and EU led initiatives).

Organisational interoperability

How would authorities (at national, Sea Basin, sectorial and European level) organise themselves to share information relevant for maritime surveillance with one another?

Each Member State appoints a single public authority that is responsible for implementing and operating a national CISE node. This node offers collects information from all public authorities within the Member State's borders and offers services using that information. The national CISE node allows offering a common integrated maritime awareness picture to CISE participants.

Public authorities can share their information by making it available in the national CISE node.

What agreements would be needed to enable authorities to share information relevant for maritime surveillance?

This vision requires cross-sectorial information sharing agreements between Member States, which could be established through interoperability agreements.

How would CISE be operated?

Service desk: A central help desk in each Member State is set up to support the users of the single Member State node. A central helpdesk at EU level is set up to support implementations of the node specifications by Member States and EU led initiatives.

Application management: Application management of the end-user system that manages connections to the authority node is dealt with at each individual authority. The application management of each national service discovery coordinator is handled on Member State level. The commonly agreed information exchange model, the node and service discovery coordinator specifications, the Common Register of Authorities, the Common Authentication Services and the Common Collaborative Platform are maintained by a central authority.

IT operations management: Authorities as information sources are responsible for respecting the interoperability agreements for accessing and providing services. It is up to each Member State authority to set up Monitoring Services used to monitor performance and to collect statistics from their node.

Technical management: Authorities and EU led initiatives are responsible for the technical management of their information systems. They can choose to use the reference node implementation or to gradually move towards the CISE specifications in their own implementation. In a similar fashion, Member States and EU led initiatives can choose to use the reference implementation of the service discovery coordinator or to gradually move towards the CISE specifications in their own implementation. The use of the CISE node and coordinator reference implementations is optional.

What kind of organizational governance needs to be established?

Member States can decide to establish a new governance level to establish and maintain the national node if no relevant governance structure already exists.

Semantic interoperability

How is information made understandable and usable?

Information is shared using a commonly agreed information exchange model, data classification levels and access profiles, catalogue of datasets and information services.

The information exchange model describes how information is structured and what controlled vocabularies and taxonomies are used to describe it; the data classification levels define a common ontology between data types and access rights; and the catalogue of datasets lists all possible CISE services.

How are access rights decided on?

Authorities manage the access rights for the information they own. If they do not own the information, they must respect the applicable licensing.

Technical interoperability

How would authorities be able to share information?

The single public authority in charge of managing the service catalogue is responsible for implementing the single CISE node by either using a reference implementation or by incrementally moving its existing systems towards the CISE node specifications. A service discovery coordinator is used by the EU led initiatives to improve the discoverability of their services; this element can also be used by Member States.

Broadcasting is enabled due to the notification service being a default service of the node specifications.

Are there specificities for national and Sea Basin authorities?

Member States authorities are responsible for the set-up and maintenance of the national node and the maintenance of the services they offer.

This vision can feature Sea Basin authorities to operate CISE nodes at sea basin level, but this would be a variation of vision C. In this case, a single integrated maritime awareness picture could be created for each sea basin. The Sea Basin authority could choose whether to use a reference implementation of the CISE node, or to gradually move towards the CISE specifications in existing systems (if applicable). The Sea Basin authority could offer any services it wishes, as long as the services comply with CISE specifications, since the same technical and semantic interoperability agreements apply to all CISE participants. The services offered by Sea Basin authorities must also be listed in the catalogue of services of the EU service discovery coordinator.

Are there specificities for EU led initiatives?

EU agencies or European Commission DGs are affected in the same manner as in vision B.

Please refer to section 6.3 for preliminary reflections on how existing EU led initiatives are impacted by

CISE. It should be noted that the existence of central systems at EU level can accelerate the setup of CISE services, as their data can be offered through CISE more easily than systems where data is scattered in local systems.

How would authorities be able to add new services?

New services are added by the single public authority that is responsible for implementing and operating the national CISE node. This authority can offer services by processing already collected information (e.g. by correlation or fusion) or by collecting information from other public authorities in the Member State or from other CISE participants (i.e. the nodes of other Member States and EU led initiatives).

How would authorities discover information relevant for them?

To discover information, a public authority consults its Member State node. The national nodes offer services including a common integrated maritime awareness picture. A service discovery coordinator is made available to facilitate the discovery of services offered by EU led initiatives.

How would authorities retrieve information relevant for them?

Authorities wishing to consume information services consult the national node of their Member State. The national node offers services using the commonly agreed messaging protocol and related specifications for data correlation and fusion.

This vision eliminates the risk of receiving similar information several times, as the services are now only offered by a single public authority that is responsible for collecting that information from the public authorities within its borders.

How are authentication and authorisation handled?

Authorisation is managed by the information providers, respecting any constraints imposed by the information owner. Each CISE participant should implement an information access management system based on the commonly agreed access profiles. Authorities are responsible for classifying their information according to the commonly agreed information classification scheme. They do not have to modify their internal classification scheme however.

The authentication of CISE participants is done through Common Authentication Services in accordance with the CISE access profiles. These services are commonly agreed and implemented by each CISE participant (as part of the node specifications) to ensure that authentication is always performed in the same manner. The use of Common Authentication Services is made possible by the standardisation of the messaging protocol. Authentication of CISE information requests and subscriptions is done at the level of the public authority. Individual end-users are not authenticated in the Common Authentication Services.

Authorities are responsible for assigning one or more CISE access profiles to their end-users. They are responsible for authenticating their end-users. When an authenticated end-user requests or sends information, their assigned CISE access profiles will be used in the information exchange.

The definition of the common services are to be defined, whether these should include specifications, reference implementation and/or services.

How is trust between participants established?

Establishing trust between the different CISE participants system can be enhanced by:

- Building a CISE security policy, specifying minimal security requirements that all CISE users and entities shall respect.
- Applying a commonly agreed classification scheme. Correct information classification by all CISE members is a key factor to prevent disclosure of information. There should be a common understanding among all CISE members about what the implications of applying information classification levels are.
- Applying commonly agreed access profiles. Following the same principles as for information classifications, there should be a common understanding of the CISE access level profiles.

How would this vision enable virtual collaboration between authorities?

Authorities can use a Common Collaborative Platform to interact with one another.

What technical governance is required?

The sustainability of CISE's technical specifications will preferably be done by standardisation bodies.

How adequate is the vision to face technical barriers?

Varying capacity of source systems to exchange surveillance and monitoring information	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
Machine-dependent, old architectures make it cumbersome to interconnect with CISE	Partly	Partly	Partly	**Fully**	Fully
Varying data quality across source systems reduces trustworthiness of CISE	Not	Not	Not	**Fully**	Partly
Varying current cross-sectorial integration of Maritime Surveillance within countries creates strong imparities in effort to connect to CISE	Not	Not	Not	**Partly**	Fully
There is a lock-in into modern commercial platform solutions	Partly	Partly	Partly	**Not**	Fully
Lack of interoperability of current systems' landscape	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
There are no common information models (as of yet)	Fully	Fully	Fully	**Fully**	Fully
There are no common technical protocols (as of yet)	Partly	Partly	Partly	**Fully**	Fully
Immature and/or diverging definition of metadata between user communities hampers cross-sectorial sharing of information	Partly	Partly	Partly	**Fully**	Fully
Data and metadata will be in different languages	Fully	Fully	Fully	**Fully**	Fully
Existing Node models will need to be integrated	Fully	Fully	Fully	**Partly**	Fully

The rating scales used are:

- Fully: the barrier is fully or to a very large extent addressed by the Vision
- Partly: the barrier is partly addressed by the Vision
- Not: the Vision is not suited for addressing the barrier.

Architectural building blocks that need to be specified[15]

Central components

Name	Volume
CISE Governance	1
Information Exchange Model	1
Register of services & authorities	1
Common Collaborative Platform	1
Common Monitoring Services	1
Reference Implementation of National Node	1
Reference Implementation of Gateway	0
Cost of connecting EU-level systems	1

Building blocks

Type	Volume
Node	26
Interface	2

[15] Definitions of components and building blocks can be found in the Glossary in Annex of this document.

SWOT analysis

What are the strengths of this vision?

Possibility to enhance the present sectorial maritime awareness pictures with additional information

The commonly agreed information exchange model and the node specifications increase commonalities in information exchanges.

Common rules for correlation and fusion of information are agreed enabling the creation of harmonised integrated maritime awareness pictures.

Member States decide what services should be in their service catalogue.

The existence of a single national authority and single national node allows the creation of integrated maritime awareness pictures at Member State level.

Concentration of resources in a single service provider could lead to economies of scale.

CapEx and OpEx are low as it is expected that both investments as well as operations are shared in Member States and redundancy is eliminated.

The Reference Implementation of the Node encapsulates standard functionalities such as common rules for aggregation & analysis, thereby increasing the quality of the Maritime Surveillance picture.

What are the weaknesses of this vision?

It requires a high level of consensus and could require a high degree of changes at in the way that the Member States are currently organised.

This Vision imposes every EU Member State to implement a National Node. This obligation may or may not fit the current Maritime Surveillance priorities and resources of the countries.

Investments may need to be made at a scale that does not correspond to the actual requirements for IT to be upgraded or replaced in the EU Member countries.

What are the opportunities associated with this vision?

A reference implementation of the node can be provided to spur adoption.

A fall-back mode based on interconnected public authorities could be considered in case of major attacks or unavailability of the national coordinator.

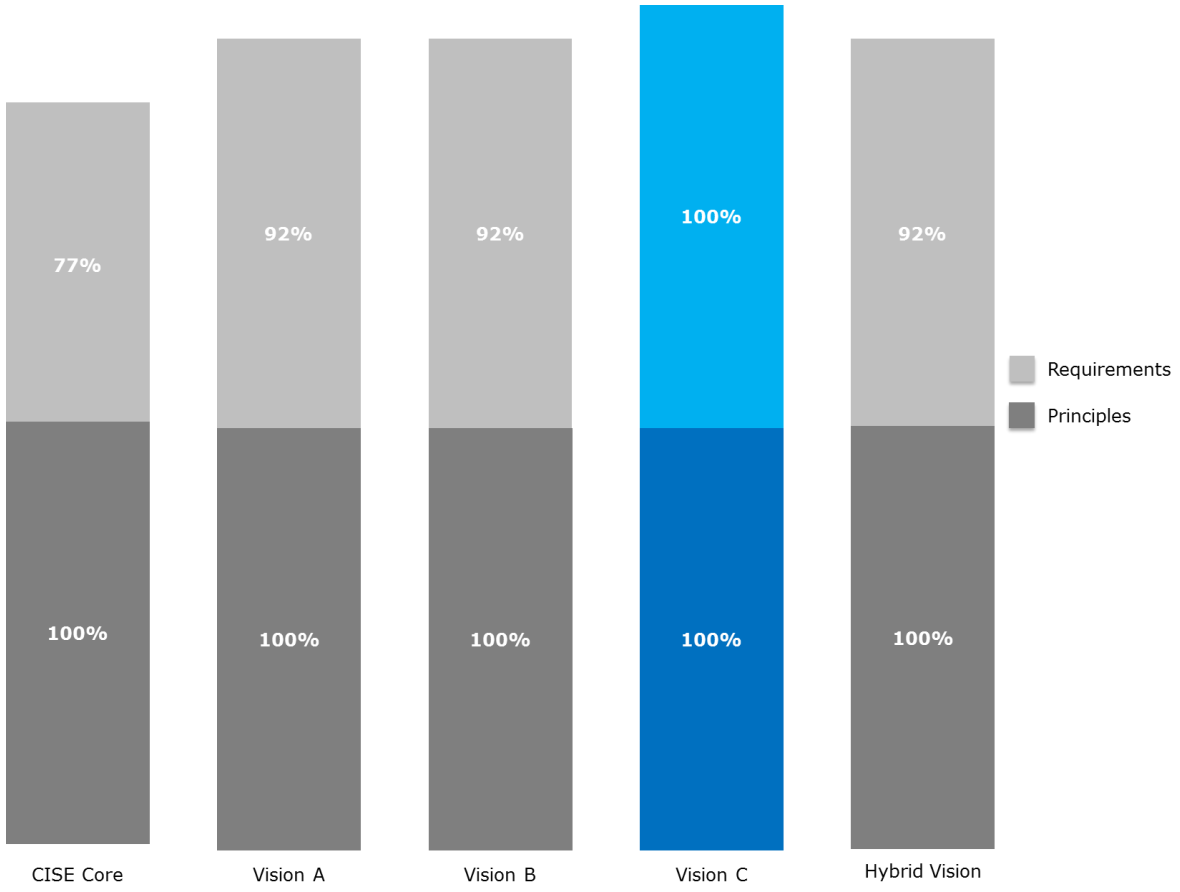
What are the threats associated with this vision?

Member States might need to establish a new national authority to manage the service catalogue and to operate the node.

A node at national level can be perceived as a single point of failure.

Selection criteria

What is this vision's effectiveness in improving maritime awareness?

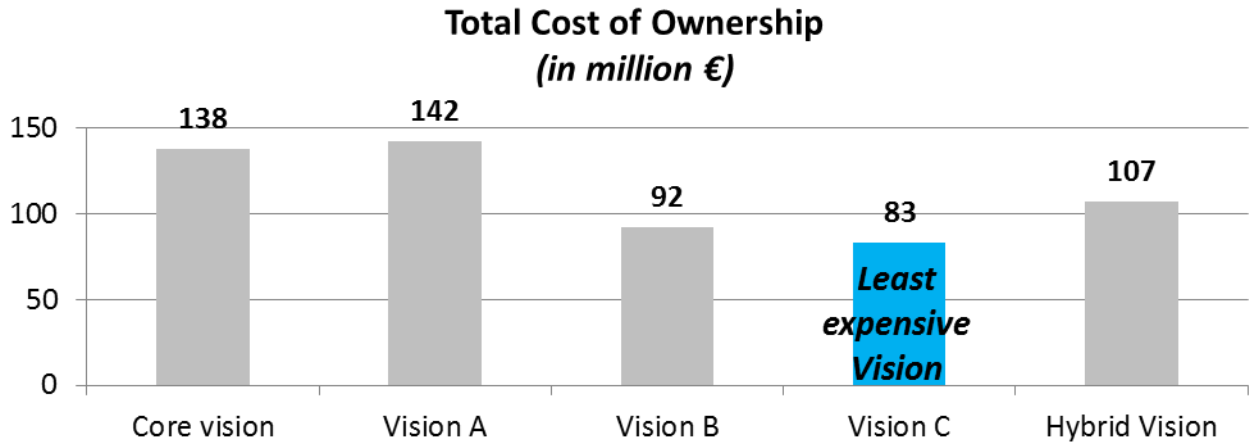


The details of the requirements coverage assessment can be found in Annex 4 .

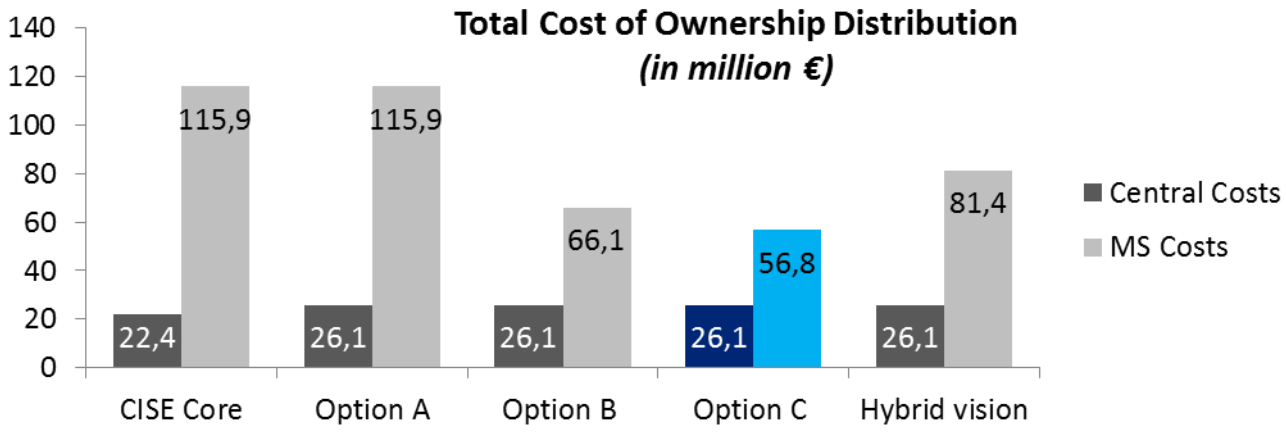
How efficient is this vision in terms of economic resources needed in the short-term?[16]

Vision C is the least expensive as expressed in Total Cost of Ownership (TOC) and, at the same time, it is the vision that fulfils all requirements.

[16] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013



Member States will bear 65% of the initial investment costs (CAPEX) and 57% of the operational costs (OPEX) calculated over 10 years.



How sustainable is this vision? What are the continued long-term benefits?[17]

At this point, the sustainability assessment results lie in the adequateness of Vision C to face technical barriers (see Technical interoperability section above).

[17] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013

Hybrid Vision – Merging Visions A, B and C (+ EU Initiatives)

The vision at a glance

Description

The hybrid vision is a merge of Visions A, B and C, created through merging the interoperability agreements of each vision. These interoperability agreements are summarised in Figure 7. Interoperability agreements are needed to ensure cross-border and cross-sector interoperability among EU Member States and EU led initiatives. The interoperability agreements table shows that Visions A, B and C already required the same interoperability agreements at semantic level and technical level. This means that these agreements can be moved to the hybrid vision as they were described in this document. The main challenge to merge the three visions is at organisational level.

At organisational level, the hybrid vision:

- Requires the appointment of 28 CISE Contact Points at Member State level, one per Member State, and 7 CISE Contact Points at EU level, one per User Community.
- Will make it possible for Member States to decide whether to nominate a single provider of CISE services at national level or multiple ones. This means that a provider of CISE services at national level may be nominated to deliver CISE services of interest for one or more User Communities. The delivery of CISE services may be done through the improvement of existing and planned systems (such as the National Single Window or National Coordination Centres).
- Requires Member States to be aware that the choice of the service delivery model will impact the content of their integrated maritime awareness model.
- More information on how the different EU initiatives fit into the hybrid vision is explained in Annex 6 .

How does this vision improve maritime surveillance?

This vision improves maritime surveillance by encouraging public authorities holding information relevant to CISE to share information with others through commonly defined semantic, technical and organisational building blocks (see what interoperability agreements are needed for this Vision below). In this vision, public authorities do not need to be aware of who provides the CISE service; this functionality will be provided by the service discovery coordinators at User Community or Member State level.

This vision promotes governance at User Community level, hence CISE participants must individually create their own integrated maritime awareness pictures by merging information collected from multiple sources. When a Member State decides to have a a single node, the national nodes are able to offer a common integrated maritime awareness picture as a service.

What interoperability agreements are needed for this vision?

At semantic level, interoperability agreements on a common information exchange model, data classification levels, access profiles, catalogue of datasets and information services are needed.

For organisational interoperability, an agreement in each User Community is needed to appoint a single

public authority in charge of managing their catalogue of services. It is likely that this agreement can rely on existing governance structures within the User Communities. Also, an agreement in each Member State is needed to appoint a single public authority in charge of managing their catalogue of services and the single provider of CISE providers. These decisions should build upon existing governance structures within the Member State.

At technical level, interoperability agreements on a messaging protocol, correlation and fusion rules, and service discovery specifications need to be made. The messaging protocol and correlation and fusion rules are implemented in software referred to as the CISE node. The service discovery specifications are implemented in software referred to as the service discovery coordinator, which facilitates the consultation of the catalogue of services and their discovery.

What changes in this vision, compared to the core vision?

Unlike the core vision, the hybrid vision:

- Requires EU Member States to designate a CISE Contact Point at national level whereas in the core vision the CISE contact point does not exist. The contact point will manage the Catalogue of CISE services so that no conflicting or redundant services are offered by the Member State or User Community.
- Requires EU Member States to designate the providers of CISE services at national level whereas in the core vision the authorities' systems are all potential providers of CISE services. The service providers will hide the organisational complexity of the Member State making the discovery and use of servicers easier.
- Requires agreements on discovery of services as well as data correlation and fusion rules.
    - Regarding fusion rules: CISE service providers will operate a CISE node to perform data correlation and fusion whereas in the core vision a CISE gateway is used. These rules are very important for the provision of information services which go beyond the exchange of “raw” information.
    - Regarding discovery of services: Organisational complexity is an important barrier to information sharing. Services need to be discovered before being used. The service discovery agreements facilitate the dynamic identification of CISE service providers.

Organisational interoperability

How would authorities (at national, Sea Basin, sectorial and European level) organise themselves to share information relevant for maritime surveillance with one another?

The hybrid vision applies a more holistic and flexible governance model that takes into consideration both the national and the User Community perspectives. The hybrid vision responds to this request by proposing a two-level governance model:

- 1st level: CISE Contact Points at Member State level to manage the catalogue of CISE services of each Member State. These are the services belonging to, and provided by, the Member States.
- 2nd level: CISE Contact Points at EU level to manage the catalogue of CISE services of each User Community. These are the services belonging to the User Communities and provided by EU led initiatives, usually, under the supervision of EU agencies. The Member States are involved in the governance of these initiatives.

It should be noted that Member States and User Communities will be able to nominate their CISE Contact Points as they see fit in line with EU's subsidiarity principle according to EU legislation if any.

The hybrid vision will require the appointment of, at least, 28 CISE Contact Points at Member State level, and, at least, 7 CISE Contact Points at EU level.

The hybrid vision is flexible about the number of CISE providers at national level. The following update is therefore proposed:

- At Member State level, CISE services may be delivered by a single service provider (as in Vision C) or by multiple ones (per User Community, as in Vision A or like Vision B in case of a different definition of User Communities).
- At User Community level, CISE services will continue to be delivered through information systems of EU led initiatives operated by EU agencies.

What agreements would be needed to enable authorities to share information relevant for maritime surveillance?

This vision may require bilateral cross-sectorial information sharing agreements between public authorities belonging to different User Communities or belonging to the different Member States.

How would CISE be operated?

Service desk: A central help desk in each Member State is set up to support the users in case of a single Member State node. In case of multiple nodes (per User Community), User Community level help desks are needed at Member State level. A central helpdesk at EU level is set up to support implementations of the node specifications by Member States and EU led initiatives.

Application management: Application management of the end-user system that manages connections to the authority node is dealt with at each individual authority. The application management of each national service discovery coordinator is handled centrally or per User Community at Member State level. The same applies for commonly agreed information exchange model, the node(s) and service discovery coordinator specifications, the Common Register of Authorities, the Common Authentication Services and the Common Collaborative Platform.

IT operations management: Authorities as information sources are responsible for respecting the interoperability agreements for accessing and providing services. It is up to each Member State authority to set up Monitoring Services used to monitor performance and to collect statistics from their node.

Technical management: Authorities and EU led initiatives are responsible for the technical management of their information systems. They can choose to use the reference node implementation or to gradually move towards the CISE specifications in their own implementation. In a similar fashion, Member States, User Communities in Member States and EU led initiatives can choose to use the reference implementation of the service discovery coordinator or to gradually move towards the CISE specifications in their own implementation. The use of the CISE node and coordinator reference implementations is optional.

What kind of organizational governance needs to be established?

The hybrid vision will make it possible for Member States to decide whether to nominate a single provider of CISE services at national level or multiple ones. This means that a provider of CISE services at national level may be nominated to deliver CISE services of interest for one or more User Communities. The delivery of CISE services may be done through the improvement of existing and planned systems (such as the National Single Window or National Coordination Centres). Both choices will, as much as possible, leverage existing governance bodies.

Semantic interoperability

Same interoperability agreements at semantic level as Visions A, B and C.

Technical interoperability

Same interoperability agreements at technical level as Visions A, B and C.

How adequate is the vision to face technical barriers to interoperability?

Varying capacity of source systems to exchange surveillance and monitoring information	**Adequateness of Vision**				
	Core	**A**	**B**	**C**	**Hybrid**
Machine-dependent, old architectures make it cumbersome to interconnect with CISE	Partly	Partly	Partly	Fully	**Fully**
Varying data quality across source systems reduces trustworthiness of CISE	Not	Not	Not	Fully	**Partly**
Varying current cross-sectorial integration of Maritime Surveillance within countries creates strong imparities in effort to connect to CISE	Not	Not	Not	Partly	**Fully**
There is a lock-in into modern commercial platform solutions	Partly	Partly	Partly	Not	**Fully**
Lack of interoperability of current	**Adequateness of Vision**				

systems' landscape	Core	A	B	C	Hybrid
There are no common information models (as of yet)	Fully	Fully	Fully	Fully	**Fully**
There are no common technical protocols (as of yet)	Partly	Partly	Partly	Fully	**Fully**
Immature and/or diverging definition of metadata between user communities hampers cross-sectorial sharing of information	Partly	Partly	Partly	Fully	**Fully**
Data and metadata will be in different languages	Fully	Fully	Fully	Fully	**Fully**
Existing Node models will need to be integrated	Fully	Fully	Fully	Partly	**Fully**

The rating scales used are:

- Fully: the barrier is fully or to a very large extent addressed by the Vision
- Partly: the barrier is partly addressed by the Vision
- Not: the Vision is not suited for addressing the barrier.

Architectural building blocks that need to be specified[18]

Central components

Name	Volume
CISE Governance	1
Information Exchange Model	1
Register of services & authorities	1
Common Collaborative Platform	1
Common Monitoring Services	1
Reference Implementation of National Node	1
Reference Implementation of Gateway	0
Cost of connecting EU-level systems	1

Building blocks

Type	Volume
Node	6
Interface	81.8

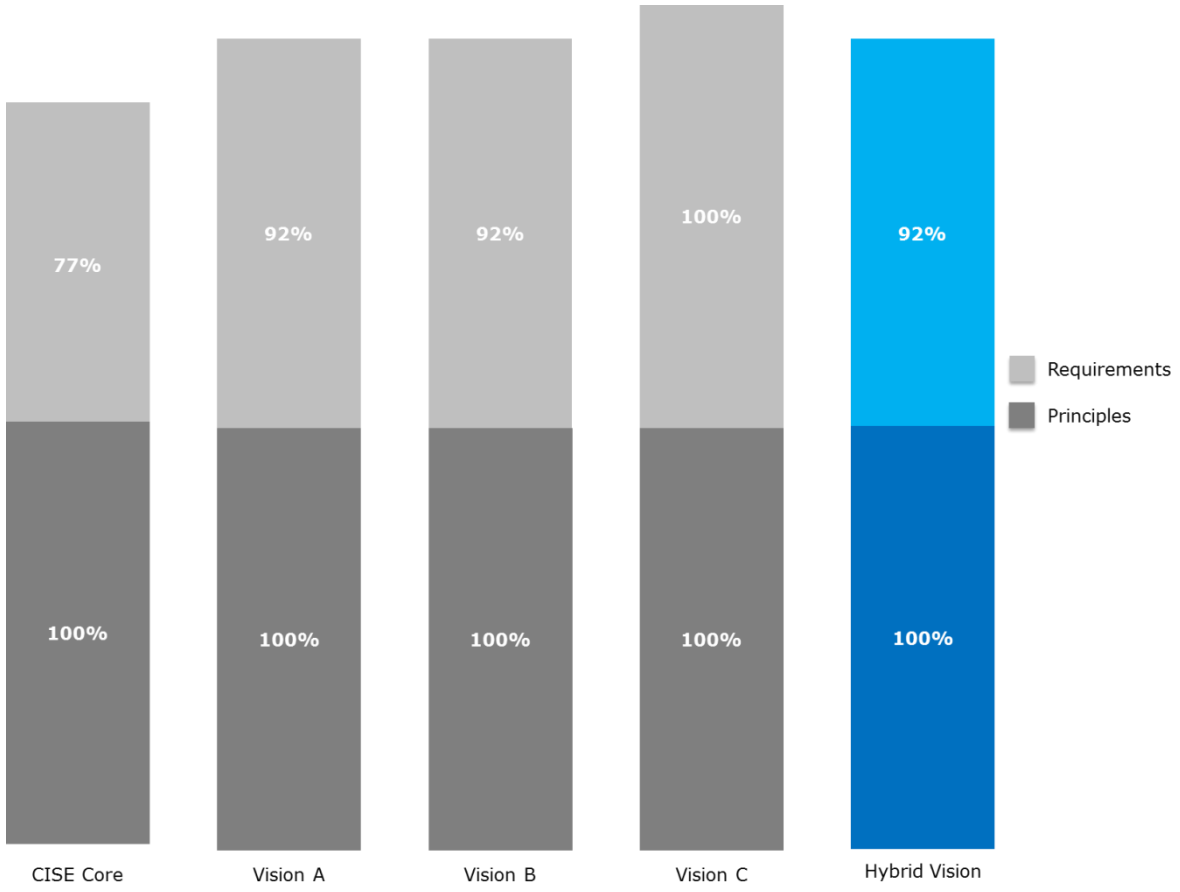
[18] Definitions of components and building blocks can be found in the Glossary in Annex of this document.

SWOT analysis

What are the strengths of this vision?	What are the weaknesses of this vision?
Governance model that takes into consideration both the national and the User Community perspectives. Flexibility on the number of CISE providers at national level. At most there should be a single CISE service provider, with a node, per User Community. However, this does not mean that there will be at most seven nodes in a Member State because some Member States may define User Communities differently. Member States maintain significant decision latitude regarding the number of service providers for CISE and can choose whom to designate as coordinator of the country's CISE services towards the EU and other Member States. Member States can implement the interconnection with CISE respecting both their current governance settings as well as their financial investment cycles.	The integrated maritime awareness model to be offered at Member State level depends on the number of CISE providers at national level.
What are the opportunities associated with this vision?	**What are the threats associated with this vision?**
A reference implementation of the node can be provided to spur adoption	Flexibility on the number of CISE providers at national level may delay decisions on how to move forward with the implementation of CISE.

Selection criteria

What is this vision's effectiveness in improving maritime awareness?

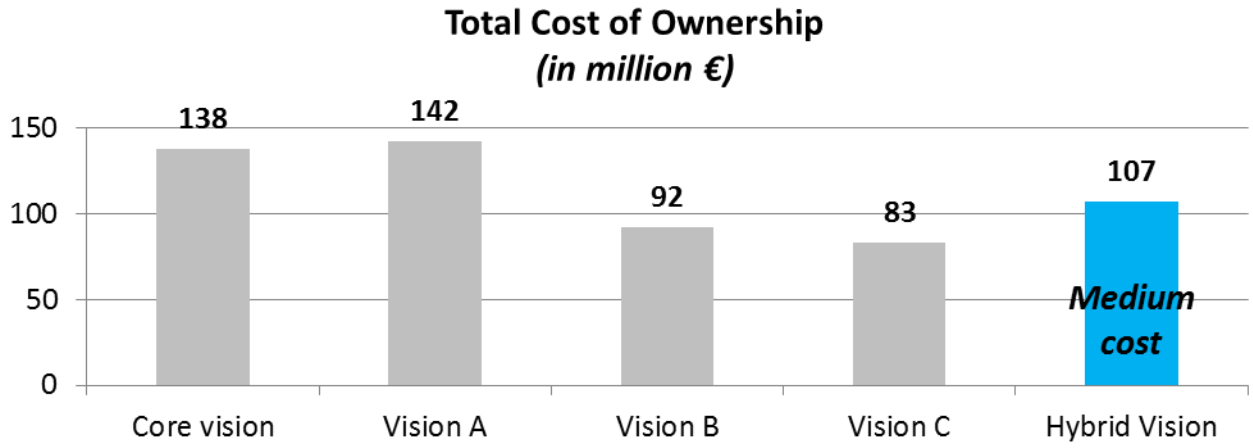


The details of the requirements coverage assessment can be found in Annex 4 .

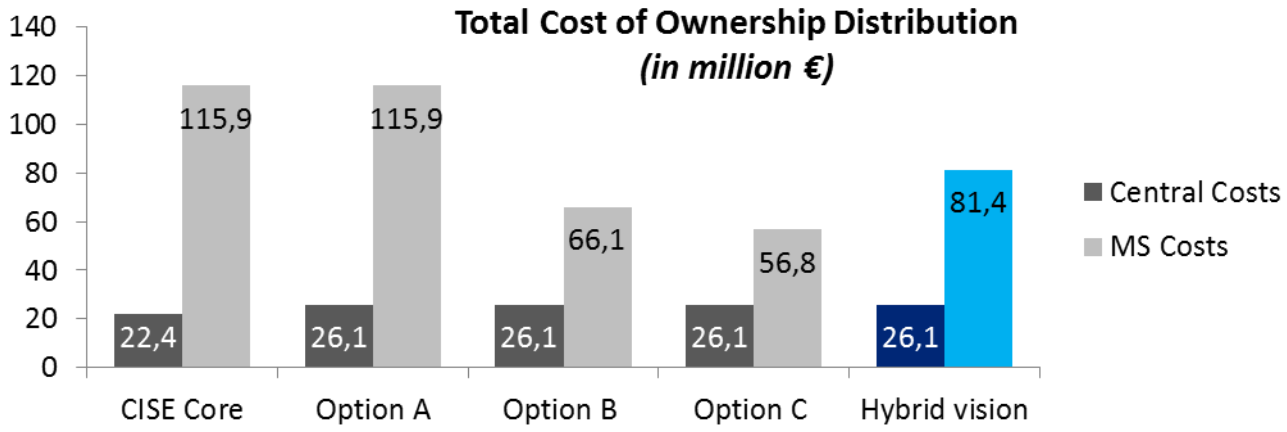
How efficient is this vision in terms of economic resources needed in the short-term?[19]

The Hybrid Vision represents a medium cost compared with other visions as expressed in Total Cost of Ownership (TOC).

[19] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013



Member States will bear 74% of the initial investment costs (CAPEX) and 65% of the operational costs (OPEX) calculated over 10 years.



How sustainable is this vision? What are the continued long-term benefits?[20]

When looking at the full set of technical barriers to CISE, the Hybrid Vision turns out to be one of the most sustainable. The Hybrid Vision tackles three out of four barriers linked to the existence of source systems with varying capacity to interconnect with CISE. The rating reflects the flexibility of this Vision in terms of the number of service providers. This vision accommodates the current set up of Maritime Surveillance environments in the Member States. Where machine-dependent, old architectures persist or authorities find themselves locked into commercial platform solutions, the Vision leaves full decision making latitude as to best connect their systems with CISE. It can in this case safely be assumed that Member States know their systems the best and are therefore the best placed to make investment and transformation choices. As result this Vision also bears a significant risk induced by the lack of an overall "national" Maritime awareness picture in every Member State.

[20] Source: *Sustainability and Efficiency of Visions for CISE*, Gartner, September 2013

6.3. How does CISE impact EU led initiatives

Depending on the vision in question, each EU led initiative has the following considerations to make in the technical, semantic and organisational areas before taking part in CISE:

1. Technical – how to move towards CISE gateway specifications (CISE CORE vision) or node specifications (Visions A-C).
2. Semantic – how to move towards CISE semantic specifications e.g. the information exchange agreement. This consideration applies to all visions.
3. Organisational – if EU initiatives feature multiple organisational levels, they need to decide whether to move towards the CISE gateway or node specifications on the Member State or EU level. This consideration applies to all visions.

The below considerations reflect a preliminary exercise to get an understanding of how existing EU led initiatives could participate in CISE. Please note that this is based on our understanding of the initiatives (refer to the Annex 2 The As-Is State of Maritime Surveillance, based on the study on the current surveillance IT landscape [9]).

- EMSA could offer or access CISE services by moving towards the CISE gateway or node specifications in their existing national applications or in the EU level nodes of SafeSeaNet, CleanSeaNet, Thetis and LRIT. Alternatively, EMSA could most likely also move towards the CISE gateway or node specifications in the IMDatE application, which provides integrated information services based on the 4 aforementioned EMSA systems. In any case, EMSA should ensure that SafeSeaNet can communicate with both the private network of SafeSeaNet and the CISE network; and follow the different interoperability agreements of CISE, including access rights.
- FRONTEX could offer or access CISE services by moving towards the CISE gateway or node specifications in one or more existing national EUROSUR nodes or in the central FRONTEX node. FRONTEX should ensure that EUROSUR can communicate with both the VPN of EUROSUR and the CISE network.
- DG HOME could offer or access CISE services within the Visa Information System (VIS) and the Schengen Information System (SIS) by moving towards the CISE gateway or node specifications in the existing national nodes or in the central EU level nodes. DG HOME should ensure that VIS and SIS can communicate with both the private network of VIS and SIS and the CISE network.
- DG TAXUD could offer or access CISE services within SPEED by moving towards the CISE gateway or node specifications. TAXUD should ensure that SPEED can communicate with both the private CCN/CSI network and the CISE network. If CISE compliant nodes are established on Member State level and vision C is chosen as the preferred vision, DG TAXUD must decide whether to let the national single node offer services on behalf of EU initiative.
- DG MARE could offer or access CISE services from the Fisheries Monitoring Centres (FMC) by moving towards the CISE gateway or node specifications in the existing national nodes of the FMCs or in the central EU Data Warehouse once it is finished. Alternatively, DG MARE could most likely move towards CISE specifications in the Data Exchange Highway for ERS data.
- DG MARE could offer or access CISE services in EMODNet by moving towards the CISE gateway or node specifications in EMODNet.

- EUROPOL could offer or access CISE services by moving towards the CISE gateway or node specifications either in the existing EUROPOL National Units or the central node of the EUROPOL Information System. Alternatively, EUROPOL could most likely move towards the CISE gateway specifications in their secure information exchange platform, SIENA. EUROPOL should make sure that SIENA can communicate with the both the private SIENA network and the CISE network.
- DG Environment and the EEA could offer or access CISE services by moving towards the CISE gateway or node specifications in the Shared Environmental Information System (SEIS) or directly in the underlying systems (e.g. the central node of the ReportNet).
- DG ENTR and its partners ESA and the EEA could offer or access CISE services by moving towards the CISE gateway or node specifications in the existing Copernicus (formerly known as GMES) node(s).
- DG ECHO could offer or access CISE services by moving towards the CISE gateway or node specifications in the existing central node of the Common Emergency Communication and Information System (CECIS). DG ECHO should ensure that CECIS can communicate with both the private network of CECIS (used for civil protection information) and the CISE network.
- The EDA could offer or access CISE services by moving towards the CISE gateway or node specifications in the existing national nodes (MEXS) of MARSUR. EDA should ensure that the MEXS can communicate with both the VPN of MARSUR and the CISE network.

The specifications of several existing initiatives could be used as inspiration for defining CISE elements e.g. the INSPIRE Directive and the Reporting Formalities Directive EU 2010/65/EU (Single National Window supported by DG MOVE) should be reused for semantic agreements (e.g. the common information exchange model). Other sources of inspiration are e.g. EUROSUR supported by FRONTEX; the Single National Window by DG MOVE; and MARSUR supported by EDA for the CISE gateway and node specifications.

Despite the preferred vision selected in the end, agencies and DGs are free to seek more integrated services through higher level cooperation and common agreements with other interested parties if they so wish.

Bibliography

[1] "REGULATION (EU) No 1255/2011 establishing a Programme to support the further development of an Integrated Maritime Policy," The European Parliament and European Council, 2011.

[2] DG MARE, "Integrating Maritime Surveillance Common Information Sharing Environment (CISE)," 2010.

[3] ISA, "European Interoperability Framework (EIF) for European public services," [Online]. Available: ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

[4] Marsuno, "Marsuno Final Report," 2011.

[5] BlueMassMed, "BlueMassMed Final Report," Secrétariat général de la mer (France), 2012.

[6] "Integrating Maritime Surveillance - draft roadmap towards estabelishing the Common Information Sharing Environment for the surveillance of the EU maritime domain," COM(2010) 584 final, 2010.

[7] European Parliament and Council, "DIRECTIVE 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC," Official Journal of the European Union, Brussels, 2010.

[8] Deloitte, "Study on the current surveillance IT landscape and resulting options," 2012. [Online]. Available: https://webgate.ec.europa.eu/maritimeforum/content/2959.

[9] European Commission, "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain," COM(2009) 538 final, 2009.

[10] European Commission, "The Limassol Declaration: Declaration of the European Ministers responsible for the Integrated Maritime Policy and the European Commission, on a Marine and Maritime Agenda for growth and jobs," European Commission, 2012.

[11] Gartner, "Sustainability and Efficiency of Visions for CISE," European Commission, 2013.

[12] ISA, "Interoperability Solutions for European Public Administrations (ISA) - Towards a European Interoperability Architecture," European Commission, 2013. [Online]. Available: http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-1action_en.htm.

[13] P. D. Dori, "Object-Process Methodology," Springer, 2002.

[14] DG MARE, "Integrating Maritime Surveillance: Communication from the Commission to the Council and the European Parliament on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain," 2010. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0584:EN:NOT.

[15] D. TAXUD, DG TAXUD, [Online]. Available: http://ec.europa.eu/taxation_customs/index_en.htm.

[16] D. CONNECT, DG CONNECT, [Online]. Available: http://ec.europa.eu/digital-agenda/en/ict-policy-support-programme.

[17] D. HOME, "DG HOME," [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/index_en.htm.

[18] I. Programme, DIGIT, [Online]. Available: http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-1action_en.htm.

[19] D. CONNECT, DG CONNECT, [Online]. Available: http://ec.europa.eu/dgs/connect/index_en.htm.

[20] IDABC, "STESTA: Secure Trans European Services for Telematics between Administrations," [Online]. Available: http://ec.europa.eu/idabc/en/document/2097.html.

[21] Council of the European Union, [Online]. Available: http://register.consilium.europa.eu/pdf/en/09/st08/st08715.en09.pdf.

[22] ISA, "Interoperability Solutions for European Public Administrations (ISA)," European Commission, 2013. [Online]. Available: http://ec.europa.eu/isa/index_en.htm.

[23] DG MARE, Draft progress report on the Roadmap to Establishing the Common Information Sharing EU nvironment ("CISE") for the surveillance of the EU maritime domain, 2012.

[24] DG MARE, "NOTE TO THE IT STEERING COMMITTEE: Integrated Fisheries Data Management (IFDM) priorities 2013," 2012.

[25] DG MARE, "LEGAL ASPECTS OF MARITIME MONITORING & SURVEILLANCE DATA (Framework Service Contract, No. FISH/2006/09 – LOT2)," 2006.

[26] DG HOME, "Policies: European Information Exchange Model (EIXM)," European Commission, 2013. [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm.

[27] EMSA, "CleanSeaNet Homepage," European Commission, 2013. [Online]. Available: http://cleanseanet.emsa.europa.eu/index.html.

[28] DG ENTR, "Copernicus: The European Earth Observation Programme," European Commission, 2013. [Online]. Available: http://copernicus.eu/pages-principales/overview/copernicus-in-brief/.

[29] IDABC, "IDABC: Archite: Projects of Common Interest: SAFESEANET," European Commission, 2009. [Online]. Available: http://ec.europa.eu/idabc/en/document/2282/5926.html.

[30] JRC, "Joint Research Centre: Blue Hub - Integrating Maritime Surveillance Data," European Commission, 2013. [Online]. Available: https://bluehub.jrc.ec.europa.eu/.

[31] E. C. F. Committee, "E-Business Possibilities for the Facilitation of Maritime Traffic: The development of Single Window in European Union Member States," European Commission, 2013.

[32] J. P. Kotter, Leading Change, 1996.

[33] ICT Policy Support Programme, "Electronic Simple European Networked Services (e-Sens," European Commission, 2012.

[34] European Commission, "iMarine: Data e-Infrastructure Initiative for Fisheries Management and Conservation of Marine Living Resources," European Commission, 2013. [Online]. Available: http://www.i-marine.eu/Pages/Home.aspx.

ANNEX 1 GLOSSARY

1.1. Defining CISE in simple terms

CISE is a collection of information sharing agreements which enable its participants to share information through interoperable digital services. These agreements formalise cooperation arrangements by clarifying, for example:

- what data is shared;
- how data is processed (transformed, correlated, merged, etc.); and
- how data is transmitted.

The aforementioned agreements are needed at organisational, semantic and technical level to remove the existing barriers obstructing information from flowing across borders and across User Communities. If these agreements are rendered binding via legislation, they would also touch upon the legal level of the European Interoperability Framework (EIF) [3].

In addition to the information sharing agreements mentioned above, a set of common services are also needed so that CISE participants are able to find each other, as well as the services that CISE makes available to them.

1.2. Other definitions

Term	Definition
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 interoperability agreement (between more than 2 authorities). May include service level specifications in the form of Service Level Agreements (refer to SLAs).
Application Programming Interface (API)	An Application Programming Interface (API) is a specification of an interface between two software components in order to make them communicate with each other.
Application	Software designed to perform specific tasks and that exposes certain functionalities through interfaces.
Architecture	The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.

Term	Definition
Architecture Building Block	A constituent of a vision that describes a single aspect of the overall vision. These elements typically describe required capability and shape the specification of Solution Building Blocks. For instance, if a Messaging Protocol is an Architectural Building Block, the SSN XML Messaging could be a viable Solution Building Block. According to Gartner, Building Blocks are composed of elementary items and form the basis of the CISE architecture. The Interface and the Node are the two Building Blocks that are the core elements in the CISE architecture.
Authority (or public authority)	Any organisation that has an interest in maritime surveillance information. An authority can be local, regional, national or European level. Throughout this document, the terms authority and public authority are used interchangeably.
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.
Capital Investment (CapEx)	According to Gartner, Capital Investment refers to the one-off cost of CISE, as opposed to on-going cost (OpEx). It is the cost of: • The following EU-level Building blocks: o Developing Information Exchange Model o Establishing Register of services & authorities o Establishing Common Collaborative platform o Establishing Common Monitoring services o Establishing Reference impl. of National Node and Gateway o Establishing Reference impl. of Gateway o Connecting EU solutions for cross-sectorial Information Exchange • The following MS-level Building blocks: o Establishing Nodes o Establishing Gateways
CISE participant	An organisation or legal entity (public authority, EU led initiative, etc.) that connects to the CISE infrastructure through a gateway or a node in order to exchange information with other participants. CISE participants are the originators and final destinations of messages.

Term	Definition
Collaboration tools	Collaboration tools refer to any piece of software that facilitates working together of two or more individuals (or authorities) to fulfil a shared, collective, bounded goal. In the context of CISE, these tools refer to audio- and video-conferencing, text-based communication (e.g. chat) and online white-boarding. Gartner makes the following distinction: **Common Collaborative Platform** Is a central application containing a set of tools allowing virtual collaboration between public authorities. These tools include secure audio, video, instant messaging and white boarding. **Common Monitoring Services** Is a set of tools that will help monitor the performance and availability of IT systems and aggregates and analyses statistics of the exchange of information including usage statistics delivered by CISE participants
Complexity	The number of relationships between elements. Acts as an information sharing barrier in technology architectures.
Confidentiality	Confidentiality is the property of maintaining the restrictions on information access and disclosure of an information item. This is often accomplished with the combination of access control and encryption techniques. Confidentiality is breached when an unauthorized individual has access to the content of an information item.
Correlation (of information)	A function where requested information from multiple sources are analysed to determine what relationships between the information exist.
Data	Facts represented in a readable language (such as numbers, characters, images, or other methods of recording) on a durable medium. Data on its own carries no meaning, but when given context, data becomes information.

Term	Definition
Efficiency	The efficiency of a vision describes how economic resources can be converted into results. Efficiency focuses on the implementation of the vision and includes the short-term costs and time required to realise the vision. This selection criterion will be based on the results of a costing study [9]. According to Gartner, it is a measure of how economically resources (cost, time) are converted into results. Efficiency first and foremost refers to the financial viability of the CISE project in terms of Total-Cost-of-Ownership through demonstrating overall investment size and investment longevity (i.e. the length of time required to execute the activities required for the investment). The characteristics of cost are important to consider in this respect: cost can for example be constant over the entire project duration; one-off, staggered; in/decreasing; possibly optional in case there are different implementation scenarios. TCO can be split into: • Capital investment (CapEx), • Operating Expenditure (OpEx) as well as its distribution over time. In the efficiency assessment, only the costs directly attributable to CISE are taken into account. These are cost that would not be incurred by the EU and/or Member States without the Common Information Sharing Environment being in place. Current and on-going investments of Member States into Maritime Surveillance to maintain and evolve operations as of today are not such directly attributable cost as they remain under Member State's budgetary competence, with full decision latitude on the Member State side as to how much to invest, when and for what purpose.
– **EU initiatives (EU-led initiatives)**	Cross-border initiatives at sectorial level.
Fusion (of information)	A function where requested information from multiple sources are blended to form a single response. Fusion of data fills information gaps and can reduce the uncertainty in information received from various sources.
Gateway	A gateway is a connecting point in a network that has two sides - one connecting to other gateways and one connecting to the CISE participant. The side of the gateway that connects to other gateways must comply with the CISE specifications as defined in interoperability agreements. The gateway can convert data and information from one protocol or format to another though the implementation of e.g. the messaging protocol and the information exchange model. According to Gartner, a **Gateway** is a sub-component of the **Interface**. It technically enables the interconnection of data through a shared boundary or physical connection between the source system and CISE.

Term	Definition
Governance	The necessary activities include governing the overall program through systematic strategic and tactical steering and establishment and maintenance of all central agreements such as Service Level Agreements with vendors and on-going contract management. It also includes dissemination activities.
Hub-and-spoke	The hub-and-spoke distribution model is a system of connections arranged like a chariot wheel, in which all traffic moves along spokes connected to the hub at the centre.
Implementation	Set of tasks at the end of which the hardware, software and procedures of the developed pilot or system become fully operational.
Information	Contextual meaning associated with, or derived from, data.
Information consumer	A role assumed by a participant to facilitate interaction and connectivity in the use of services.
Information exchange model (IEM)	A logical representation to illustrate the structure, semantics, and relationships of information. According to Gartner*, an* **Information exchange model** is the core of CISE and establishes a syntactic and semantic model for the exchange of Maritime Surveillance information and enables CISE to follow a decentralized approach whereby public authorities are able to work in an interoperable manner, based on common semantic standards.
Information owner	A user who ensures the consistency and validity of information. They define the security needs of the information for which they are responsible. Information ownership means identifying which participants have the right to change information, together with their obligation to determine impact and notify all impacted parties. Typically, each authority as the owner of its information may define the rules for access to its information.
Information provider	A role assumed by a participant to facilitate interaction and connectivity in the exchange of information.
Information service	An information service is a part of an information system. By exposing a service, information owners can share information stored and/or managed within their information system with others.
Information source	Authentic provenance of the information.
Information system	An information system consists of a well-defined set of data, software, hardware, telecommunications, and organisational procedures which provide information and associated functions to specific groups of users so as to ensure the efficient and effective execution of the organisation's operational, tactical and strategic tasks.

Term	Definition
Integrated maritime awareness picture	For the purpose of this document, "integrated maritime awareness picture" is defined as a "picture" produced by means of collection, analysis, interpretation and visualisation – when appropriate through a graphical interface – of data and information received from and shared with different authorities, platforms and other sources in order to achieve maritime awareness and to support the reaction capability at sea.
Integrity	Integrity is the property of maintaining the completeness, accuracy and validity of an information item during the life of the item. This is often accomplished with checksums, cryptographic hash functions, message authentication codes (MACs) and digital signatures. Integrity is breached when an unauthorized individual is able to modify the information item (data file or information exchange) without being noticed.
Interface	Interfaces make data sets available to CISE.
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.
Interoperability agreements	Means of reaching consensus on a common information sharing interface (also referred to as service interface) through which services can be offered. There are 4 different types of interoperability agreements: legal, semantic, technical and organisational.
Interoperability framework	An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.
Intricacy	The state of containing a large number of parts or details. Acts as an information sharing barrier in technology architectures.
Lightweight Directory Access Protocol (LDAP)	LDAP is a standard protocol for accessing and maintaining distributed directory information services over an IP network. It is often used to manage access rights.
License	A licence is a document containing provisions allowing or restricting actions and uses normally reserved for the copyright holder.
Multicasting	A type of message distribution where a message is sent to a number of specific members, of a group such as a department or enterprise.

Term	Definition
Node	A CISE node is a connection point in the CISE network which implements the specifications of the messaging protocol. In addition it complies with the specifications of the correlation and fusion rules. According to Gartner, a Node holds information from numerous, cross-sectorial information sources of different authorities. The Node pre-processes this information (e.g. through correlation, fusion, aggregation) with the help of integrated intelligence capabilities. The information can be complemented with meta data such as quality, provenance etc. The Node includes a gateway and a translator. The Node makes information available to other CISE Gateways. The Node supports the exchange of files of varying size and formats. The Node includes security and monitoring capabilities as well as registry capabilities to facilitate the management of a large number of data sets and services for different users. The Node requires some type of organization and governance structure in order to manage it.
Notification	A service that can be used to inform many authorities at once (e.g. by multicast or by broadcast).
Operating Expenditure (OpEx)	According to Gartner, Operating Expenditure refers to the on-going cost of CISE, as opposed to the one-off cost (CapEx). It is the cost of: • The following EU-level Building blocks: o CISE governance o Maintaining Information Exchange Model o Operating and maintaining Register of services & authorities o Operating and maintaining Common Collaborative platform o Operating and maintaining Common Monitoring services o Operating and maintaining Reference implementation of National Node and Gateway o Operating and maintaining Reference implementation of Gateway o Operating and maintaining interconnections of EU systems • The following MS-level Building blocks: o Operating and maintaining Nodes o Operating and maintaining Gateways
Payload	The essential bits of data that are being carried within a message “packet”. The payload does not include the “overhead” data required to get the packet to its destination.
Public Key Infrastructure (PKI)	A Public Key Infrastructure (PKI) is the set of hardware, software, people, policies and procedures needed to create, distribute, use, store and manage digital certificates used for data encryption.

Term	Definition
Principle	They provide for a high level design rationale, which must always be taken into account when creating, changing or removing any CISE-related element.
Proportionality	Similarly to the principle of subsidiarity, the principle of proportionality regulates the exercise of powers by the European Union. It seeks to set actions taken by the institutions of the Union within specified bounds. Under this rule, the involvement of the institutions must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued. The principle of proportionality is laid down in Article 5 of the Treaty on European Union. The criteria for applying it is set out in the Protocol (No 2) on the application of the principles of subsidiarity and proportionality annexed to the Treaties.
Protocol (or messaging protocol)	A set of procedures in information exchange that the authority systems or nodes use to send messages back and forth. Networks and systems cannot communicate unless they use the same protocol or make use of a node.
Query	A request for information retrieval within the database of an information system.
Reference implementation	A reference implementation is an implementation of CISE's specifications to be used as the standard, against which other implementations can be compared. It verifies that the specifications of CISE are implementable. The use of the CISE reference implementations is optional. According to Gartner, the reference implementations support all key functionalities of the actual implementation and are distributed to CISE participants for re-use.
Register of services & authorities	Is a directory containing the list of services and contact details of CISE participants
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.
Requirement	Determine the expectations of the stakeholders with regards to information sharing and discovery, information assurance and security, collaboration, organisation, etc.
S-TESTA	A private EU network supporting the exchange of information up to the security level of 'EU RESTREINT'.
Sea Basin	This refers to the following sea regions: Baltic Sea, Black Sea, Mediterranean Sea, North Sea, the Atlantic and the Arctic Ocean.

Term	Definition
Service	A unit of functionality that an authority exposes to other participants of CISE. These services are accessible through a service interface.
Service consumer	A service consumer refers to any information system that uses a service exposed by some other information system (called the service provider).
Service discovery coordinator	The service discovery coordinator facilitates the dynamic identification of service providers. It provides a standardised interface where gateways or nodes can retrieve information about the services provided by CISE participants. The term "information" is here used in its broadest and most general meaning – it may be information about anything from supported document types or User Communities to specific information about message exchange protocols and technical endpoint addresses. The interaction between the service discovery coordinator and the gateway or node is completely automated.
Service interface	A point of access where a service is made available to another application.
Service Level Agreement (SLA)	A service-level agreement (SLA) is a contract between an information provider and an information consumer that specifies, usually in measurable terms, what services the information provider will furnish. Some metrics that SLAs may specify include: What percentage of the time services will be available; The number of users that can be served simultaneously; Specific performance benchmarks; and Help desk response time.
Service Oriented Architecture (SOA)	A Service-Oriented Architecture (SOA) is a set of principles and methodologies for designing and developing software in the form of services. These services are well-defined business functionalities that are built as software components (discrete pieces of code and/or data structures) that can be reused for different purposes. SOA design principles are used during the phases of systems development and integration.
Service provider	A service provider is an information system that makes available a service to others. When exposing a service, the service provider defines how the service must be used by others (called service consumers). The user of the service only needs to comply with these definitions; the internal workings of the service (e.g. how information is stored, processed or where it originates) are hidden from the user.
Solution Building Block (SBB)	Represent the actual components that will be used to implement the required capability. For instance, if a Messaging Protocol is an Architectural Building Block, the SSN XML Messaging could be a viable Solution Building Block.

Term	Definition
Standard	The description of the detailed minimum requirements for procedures and methods to be implemented.
Subscription	An agreement between the information provider and the information consumer for providing, receiving or making use of information in a continuing or periodic nature.
Subsidiarity	The principle of subsidiarity aims at determining the level of intervention that is most relevant in the areas of competences shared between the EU and the Member States. This may concern action at European, national or local levels. In all cases, the EU may only intervene if it is able to act more effectively than Member States.
Sustainability	The sustainability of a vision describes the probability of each vision to realise continued, long-term benefits and the long-term costs that are incurred. It focuses on operating CISE in the long-term. This selection criterion will be based on the results of a costing study [18]. According to Gartner, sustainability refers to the sustainability of the IT environment underlying CISE. This is expressed in the future environment's ability to present an evolving life-cycle in the face of: changing requirements, changing technologies, the environment's capability to overcome technological barriers, the manageability of resource allocation to operate & evolve IT systems, the environment's capability to ensure maximum activity and attract new participants and IT systems' portability in terms of ease of implementing and adapting CISE concepts and approaches to other (pan-European) environments. The probability of continued long-term benefits happens once major initial investments have been completed (resilience to risk on the net benefit flows over time).
System	In general, a system is any integrated composite of people, information, products, applications, services, infrastructure and processes that provide a capability to satisfy a stated need or objective.
Total-Cost-of-Ownership (TCO)	All types of cost (IT as well as non- IT: electricity, floor space, personnel etc.) are reflected rather than providing a mere IT-centric budget. Cost are calculated for either the entire life-cycle or budgeting period of the project (e.g. 10 years in the case of the Cost Model at hand). By taking such a holistic view, the TCO calculation considerably reduces the risk of having to bear additional cost to the owner of an ICT project once budgets have been finalized and allocated to the initiative. TCO is a concept created by Gartner.
Translator	Data exists in a number of different legacy formats that need mapping to the CISE Information Exchange Model. According to Gartner, the translator guarantees conformity of data with the CISE Information Exchange Model. The translator translates between the legacy and CISE's Information Exchange Model.

Term	Definition
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.
Virtual Private Network	A virtual private network (VPN) is a private and secure network that connects remote users and networks within a larger public network such as the internet as if they are connected via a dedicated network. Security in a VPN is realised through tunnelling protocols and encryption.
Web service	A web service is a method or means to exchange information between electronic devices (machine-to-machine) over the internet.
White boarding	The use of modern technologies to share images, maps and documents on the screens of different (geographically dispersed) computers. It allows people to work on the same image, map or document at the same time, each seeing the changes made by others in real time.

1.3. Acronyms of European Entities

European Entities	Definition
DG ECHO	Directorate-General for Humanitarian Aid and Civil Protection
DG ENTR	Directorate-General for Enterprise and Industry
DG HOME	Directorate-General for Home Affairs
DG MARE	Directorate-General for Maritime Affairs and Fisheries
DG MOVE	Directorate-General for Mobility and Transport
DG TAXUD	Directorate-General for Taxation and Customs Union
DIGIT	Directorate-General for Informatics
EDA	European Defence Agency
EEA	European Environment Agency
EMSA	European Maritime Safety Agency
ESA	European Space Agency
EU	European Union
EU LRIT CDC	European Union Long-Range Identification and Tracking Cooperative Data Centre
EUROPOL	European Police Office
EUROSUR	European Border Surveillance System
FMC	Fishing Monitoring Centre
JRC	(Directorate-General for) Joint Research Centre

1.4. Other acronyms

Acronym	Definition
AIS	Automatic Identification System
API	Application Programming Interface
CCN/CSI	Common Communication Network and Common Systems Interface
CECIS	Common Emergency Communication and Information System
CISE	Common Information Sharing Environment
C-SIS	Central Schengen Information System
DEH	Data Exchange Highway
DWH	Data Warehouse
EIF	European Interoperability Framework
EMODNet	European Marine Observation and Data Network
ERS	Electronic Reporting System
ENU	European National Unit (EUROPOL)
GMES	Global Monitoring for Environment and Safety
IFDM	Integrated Fisheries Data Management program
IMDatE	Integrated Maritime Data Environment
INSPIRE	Infrastructure for Spatial Information in the European Community (directive)
IP	Internet Protocol
ISA	Interoperability Solutions for European Public Administrations [22]
LRIT	Long-Range Identification and Tracking
MARSUR	Maritime Surveillance (project by EDA)
MEXS	(National Node of MARSUNO)
MIC	Monitoring and Information Centre
MSEsG	Member States' Expert sub-Group (on the Integration of Maritime Surveillance)
N-SIS	National Schengen Information System
NCC	National Coordination Centre (of EUROSUR)
SAR	Synthetic Aperture Radars
SEIS	Shared Environmental Information System
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System

Acronym	Definition
SSL	Secure Sockets Layer
sTESTA	Secure Trans-European Services for Telematics between Administrations
TAG	Technical Advisory Group
VIS	Visa Information System
VMS	Vessel Monitoring System
VPN	Virtual Private Network
XML	Extensible Mark-up Language

ANNEX 2 THE AS-IS STATE OF MARITIME SURVEILLANCE

Since one of the founding principles of CISE calls for the reuse of existing tools and technologies in maritime surveillance (refer to chapter 4 Principles of CISE), a study on the current surveillance IT landscape was conducted by a contractor last year (2012). The objectives of this study included e.g. ensuring a better understanding of the initiatives and projects that could potentially be reused in view of establishing CISE; and to perform technical analyses of a set of information systems for information availability and exchange [8]. This study mainly focused on large scale EU led initiatives.

As a result of the aforementioned study and the work performed by the TAG, it has been concluded that EU level initiatives only cover a part of the information exchanged – a considerable amount of information still remains in national systems. [23] Barriers to information exchange across borders and sectors are exhibited in several areas - legal, technical, semantic and organisational. This is why interoperability agreements are needed in these areas to overcome the barriers, as explained in section 3.1 Understanding the different architecture visions. While this Architectural Vision document prescribes different sets of Architectural Building Blocks to overcome organisational, semantic and technical barriers; the CISE impact assessment will focus on legal barriers.

The sections below give a high-level summary of the structure of each User Community, based on the study on the current surveillance IT landscape mentioned above. Please note that only EU level initiatives were taken into account and that the initiatives mentioned below do not constitute an exhaustive list of maritime surveillance initiatives in Europe.

For a description on how User Communities would be impacted by the selection of a certain vision, please refer to the visions themselves in chapter 6 Architecture visions of CISE. All visions include a section that elaborates on the impact of each vision on User Communities initiatives.

1. CURRENT USER COMMUNITY INITIATIVES

1.1. Border Control

The main initiatives in the Border Control User Community are:

- **EUROSUR -** The European Border Surveillance System (EUROSUR) provides a platform to cooperate and to share operational information in the form of structured messages about external border events (e.g. illegal immigration, organised crime, drug trafficking, customs fraud, etc.) that are of common interest. EUROSUR is a decentralised network of identical national nodes called National Coordination Centres (NCCs). Each NCC collates information from various border control and law enforcement bodies to create a coherent national picture. NCCs are connected to each other and FRONTEX over a secured internet connection (VPN). EUROSUR itself does not process raw data; therefore, a set of resource projects were set up, namely SeaBilla, PERSEUS and I2C, to extending the capabilities of the EUROSUR network. EUROSUR is managed by FRONTEX. [8]
- **VIS** – The Visa Information System (VIS) allows the exchange of VISA data between Schengen States. This system facilitates the exchange of information related to visa applications made, conditions attached and visas granted, in order to help combat fraud, to identify persons no longer eligible for entry, to improve internal security of Member States etc. The architecture of the system consists of the central system (CS-VIS) providing central capabilities and data storage; and the national interface (NI-VIS) allowing participating countries to connect their national VISA systems to the central VIS

system. The system-to-system interface is based on web services over the secured network sTESTA. VIS is managed by DG HOME. [8]

1.2. Customs

The main initiative in the Customs User Community is:

- **CCN/CSI (e-Customs) –** With e-Customs, the European Commission and the Member States are committed to set up and operate secure, integrated, interoperable and accessible customs computerised systems. The EU-prescribed private communications network between Member States and the European Commission is the Common Communication Network and Common Systems Interface (CCN/CSI), which consist of a physical gateway and a set of protocols and application programming interfaces. CCN/CSI is managed by DG TAXUD. [8]

1.3. Fisheries Control

The main initiatives in the Fisheries Control User Community are:

- **IFDM** – DG MARE's Integrated Fisheries Data Management (IFDM) program contributes to the 2020 vision by establishing an integrated European information system for fisheries management. The main deliverables of the IFDM include the Data Exchange Highway (DEH), ERS and the Data Warehouse (DWH) projects, which form the basis for the current data exchange and reporting system. DEH consists of a central node, which channels the connections between different end points. The automated data exchange via the DEH is secured via 2-way SSL. Member States use the DEH to exchange ERS data between Member States and to perform their monthly reporting on aggregated fisheries control data to the European Commission. This data forms the basis for long term statistics, maintained in the DWH. [8], [24]
- **VMS and ERS** – The Vessel Monitoring System (VMS) and the Electronic Reporting System (ERS) are two separate systems used to exchange data over satellite communications from fishing vessels to the national Fisheries Monitoring Centre (FMCs). The VMS is the primary monitoring tool for national authorities to track the movements of its fishing vessels e.g. location, speed and course of vessels. VMS data is exchanged over secured https connection. The ERS is designed to enable the collection, storage and exchange of fishing activity data (e.g. aggregated catches, sales etc.). Fisheries legislation defines reporting obligations, content and format; but the technical solutions for implementation are up to Member States. The basic principle is that vessels report to their flag state, which forwards the information to the other states if necessary (e.g. if vessel is in the waters of another Member State). [8], [25].

1.4. Defence

The main initiative in the Defence User Community is:

- **MARSUR** – The aim of this initiative is to improve the maritime picture by linking existing military networks and systems to foster information exchange between all voluntary participants. MARSUR is a decentralised network, whereby existing national systems are connected to a national node (MEXS) through an API interface over a secured internet connection (VPN). The MEXS provides common services/capabilities to enable data exchange, such as chat, notification, email, track exchange, white boarding, file sharing, etc. Services can be both distributed and central. The exact data shared can differ from Member State to Member State and from case to case, based on the bilateral and

multilateral agreements between the Member States. MARSUR is managed by the European Defence Agency (EDA). [8]

1.5. Law Enforcement

In main initiatives in the Law Enforcement User Community are:

- **EUROPOL Information System and SIENA** – EUROPOL's Secure Information Exchange Network Application (SIENA) is the platform for the exchange of operational information concerning international crime between the European Police Office (Europol) and its partners. Europol exchanges data with Member States through the Europol National Units (ENUs), which in turn have access to relevant national data. The Europol systems are interconnected, which means that all information inserted into one system can also be identified in the others. SIENA itself is a central web-based application offering generic front-end and back-end functionality for structured messaging and case management through a secured web interface over sTESTA. SIENA is physically located in the Europol Data Centre in The Hague. The next steps for developing SIENA involve a system-to-system interface to access the system based on web services. [8]
- **SIS II and SIRENE –** The Schengen Information System (SIS) allows national border control and law enforcement authorities to exchange information on the cross-border movement of persons and goods. The Central Schengen Information System (C-SIS) is located in Strasbourg (France) and it collects stores and redistributes alerts submitted by participants (e.g. alerts on missing persons or for refusal of entry). Member States can access alert information by installing a National Schengen Information System (N-SIS) to connect to the C-SIS, or by directly connecting to the C-SIS using available API. N-SIS agents have read-only access. The creation, updating, follow-up and deletion of operations on SIS records are done by each Member State's SIRENE bureau (Supplementary Information Request at the National Entries) or other competent authority depending on state. SIS uses secure network sTESTA. The SIS and SIRENE are managed by DG HOME. [8] [26]

1.6. Marine Environment

The main initiatives in the Marine Environment User Community are:

- **INSPIRE** – The Directive on Infrastructure for Spatial Information in the European Community (INSPIRE) was passed in 2007 to support policies and activities, which may have an impact on the environment. The Directive addresses 34 spatial data themes, which come with common Implementing Rules (IRs). [8]
- **EMODNet** – The European Marine Observation and Data Network (EMODNet) has as goal to create a network where maritime observation data can be shared openly. In EMODNet the maritime observation data is split into 6 datasets, each having its own pilot web portal. The two main capabilities offered by the EMODNet portals are the queries it provides into the databases of the Member States and the Data Products correlating the available data into a combined picture. Data can also be exchanged in between the portals using web services. EMODNet is managed by DG MARE. [8]
- **SEIS –** The aim of the Shared Environmental Information System (SEIS) is to improve the collection, exchange and use of environmental data in Europe. SEIS is a decentralised system composed of several, interconnected systems and initiatives managed or supported by the DG Environment, EEA, JRC, Eurostat and the Member States themselves. One of the key systems in SEIS is ReportNet, an electronic reporting system with central EU storage. Two other important initiatives, in which SEIS is

involved, are Eye On Earth (public website to access environmental information services) and Wise Marine (a set of agreements between the European Commission and the participating States on the capturing, reporting and sharing of marine environmental data). [8]

- **CleanSeaNet** - CleanSeaNet is a satellite-based oil spill monitoring and vessel detection system using satellite surveillance. The images captured by Synthetic Aperture Radars (SAR) are transmitted to the nearest ground station, where they are processed and interpreted by experienced image analysts. Once the satellite images have been analysed by the service providers, they are sent to CleanSeaNet. If an oil spill is detected, alert information will be sent by CleanSeaNet to the pollution control authorities of Member States. On top of oil spill alerts, CleanSeaNet also provides slick position and shape, as well as wind and wave data. Member States can access the application via the web-based portal or via a system-to-system interface using web services. Vessels appearing in satellite images can be identified by correlating the satellite data with AIS data from SafeSeaNet. CleanSeaNet is a central system with an EU level database, which is hosted and managed by the European Maritime Safety Agency (EMSA). [8], [27]
- **Copernicus (previously known as GMES)** – Copernicus is a European system for monitoring the Earth. It collects data related to the environment and security from multiple sources, such as earth observation satellites and in situ sensors e.g. ground stations, airborne and sea-borne sensors. Most information provided will be as open as possible and most of the information services will be accessible online. Copernicus has a central portal serving as the single access point to informational services processing data from the various systems and sensors. The Copernicus programme is coordinated and managed by the European Commission (DG Enterprise and Industry). The development of the observation infrastructure is performed under the aegis of the European Space Agency (ESA) for the space component and of the European Environment Agency (EEA) and the Member States for the in situ component. [28]

1.7. Maritime Safety and Security

The main initiatives in the Maritime Safety and Security User Community are:

- **SafeSeaNet** – SafeSeaNet is a European platform for maritime data exchange with the aim of helping prevent marine pollution and accidents at sea. It is an internet based system with distributed databases. The main type of data exchanged via SafeSeaNet is Automatic Identification System (AIS) data, which includes vessel name, flag, vessel type, dimensions etc. In addition to AIS data, four types of information services are distinguished: ship notifications, incident reports, port notifications and hazmat notifications. Each Member State must assign a national competent authority to run a national node, which collects data from existing national and regional systems. Upon an information request, the central SafeSeaNet European Index Server (a hub-and-spoke) aggregates information and distributes it back to the requesting Member State according to the national user rights. SafeSeaNet is managed by the European Maritime Safety Agency (EMSA) and DG MOVE. SIS uses secure network sTESTA. [8], [29]
- **LRIT** –The Long-Range Identification and Tracking (LRIT) of all EU flagged vessels is performed worldwide by the EU LRIT Cooperative Data Centre (CDC). The EU LRIT CDC is hosted and managed by EMSA, under the leadership of DG MOVE. The EU LRIT CDC is a central application taking care of capturing, storing and distribution of LRIT data with other international LRIT data centres globally. Equipment on board of vessels automatically submits ship identification and position data via satellite to the EU LRIT CDC, from where it can be accessed by the Member States. Each State has to nominate

a National Competent Authority for LRIT, which will assign the user roles and access rights to all relevant national authorities. Access is realised via a web portal or via an XML-based system-to-system interface, but a fixed IP address is needed. The EU LRIT CDC provides flag reports to SafeSeaNet. [8]

- **Thetis** - Thetis is a central, web-based system, which supports the new Port State Control inspection regime by facilitating the planning, logging and publishing of vessel inspections. Member States access the system via the LifeRay web portal (https). Data regarding the results of inspections are stored in a central databases located in the European Maritime Safety Agency (EMSA) Data Centre in Lisbon (Portugal). To facilitate the planning of ship inspections, Thetis is linked to SafeSeaNet for vessel traffic information and to AROS to get updates on required vessel certificates. [8]
- **IMDatE –**The Integrated Maritime Data Environment (IMDatE) project is managed by EMSA under the leadership of DG MOVE. IMDatE is an integrated platform that aims to support and enhance the existing EMSA applications (SafeSeaNet, CleanSeaNet, LRIT and Thetis), by integrating the information gathered (AIS, LRIT, SAR, etc.) and processed by these systems to provide new more complete services (e.g. AIS data combined with LRIT). The new functionalities will include more visions for data visualisation, a single sign-on process, new machine-to-machine interfaces and automated vessel behaviour monitoring. Data quality will also improve, for example, through the confirmation of vessel details across different vessel registries. IMDatE uses secured internet access via https and access rights are based on those determined by the underlying systems. [8]
- **CECIS –** CECIS is a web-based alert and notifications application to support the European Monitoring and Information Centre (MIC) in mobilising civil protection and marine pollution resources from participating States in case of an emergency (e.g. a natural, technological, radiological or environmental accident). CECIS is a centralised system with centralised data. It allows users to send structured messages via a web portal. Two versions of CECIS exist, one for exchanging data about marine pollution (using the internet) and one for exchanging classified information regarding civil protection (using sTESTA). CECIS is managed by DG ECHO. [8]

1.8. Cross-User Community initiatives

The main initiative concerning all User Communities is:

- **Blue Hub –** Blue Hub is an initiative led by JRC to build a data prototype platform for the collection, integration and analysis of global, regional and local data with the aim to improve the creation of integrated maritime surveillance pictures. Main capabilities include:
    - data gathering and ingestion from various sources (AIS, LRIT, VMS etc.);
    - multi-target tracking for the fusion of data;
    - estimation of an innovative maritime situational picture by the prediction of vessel positions driven by contextual information, such as traffic routes, land avoidance, port positions etc.;
    - correlation of VDS targets with the vessel tracks fused from the various sources;
    - generation of traffic densities and risk maps. [30]

- **Single Window in European Union Member States -** Following the approval of the *Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the European Union Member States*,

the electronic submission of the reporting formalities in electronic format via a single window will enter into force by 1 June 2015. The national single window will allow ships and their representatives to submit reports to the competent authorities in electronic format and to submit individual information only once. To maximise the benefits of this development, DG MOVE and EMSA have expressed their intent to link information systems already established within the EU, such as the SafeSeaNet and the e-Customs. [7] [31]

ANNEX 3 RECOMMENDATIONS FROM CISE PILOT PROJECTS

The following table summarises the recommendations coming from the two CISE pilot projects BlueMassMed [5], which took place in the Mediterranean sea, and the MARSUNO [4], which took place in the northern sea basins. Recommendations are drawn from the following areas:

- Governance;
- Common awareness;
- Data classification levels;
- Standardisation; and
- Common services.

On the right hand side we can see how these recommendations can be mapped to the CISE core and the three visions, the blue box indicating that the recommendation has been taken into account in a given vision.

	Recommendations coming from BlueMassMed	**Recommendations coming from MARSUNO**	**Map to visions**	
Regarding Governance	(...) interoperable network that can be exploited at the same time for sectorial and cross-sectorial information services exchange among competent authorities and European agencies, according to a data distribution and access policy that will result from the combination of constraints enforced by: - relevant sectorial coordination bodies, as far as the sectorial dimension of the data exchange is concerned; - national coordination bodies, as far as the sensitivity and national security dimension of the data exchange is	To establish an effective CISE demands an overall administrative handler function to be established, with clear responsibilities and legal authorisation organised nationally.		**Core**
			■	**Vision A**
			■	**Vision B**

	Recommendations coming from BlueMassMed	Recommendations coming from MARSUNO	Map to visions	
	concerned; - future EU coordination bodies, as far as the general cross-sectorial cross-border data exchange policy is concerned (enforcing a "need-to-share" and "responsibility-to-share" paradigm). Subsequently, one main recommendation from the BMM project is to proceed with the project definition phase, based on the achieved technical results, and keeping at government/institutional level the design authority, (...).		■	Vision C
Regarding the common awareness picture	To prolong the BMM achievements and to consolidate the Shared Basic Common Maritime Picture (SBCMP) concept as the key feature enabling cross-sectorial/cross border decision support capabilities on the C.I.S.E., further harmonization of maritime picture information fusion techniques and standardization of the related operational procedures deserves to be pursued at national (inter-ministerial) level and then at EU level, with corresponding governance schemes at national and EU level, in compliance with the applicable operational and legal constraints.			Core
				Vision A
			■	Vision B
			■	Vision C
Regarding data classification levels	Define a Data Distribution Plan (DDP) in a cross-sectorial landscape, in compliance with the legal framework, to determine the rules to apply in exchanging information, considering the different categories of data (basic, personal, commercial, sensitive, confidential) and the operational sectors;	To safeguard a reliable level of quality of information, Member States should reach agreement on classification levels regarding exchange of information. The Member States should define common security requirements. Exchange at a non-classified level should be encouraged and 'over-classification' of information should be avoided.	■	Core
			■	Vision A

	Recommendations coming from BlueMassMed	Recommendations coming from MARSUNO	Map to visions	
				Vision B
				Vision C
Regarding standardization	Develop Standards for data dissemination (format, exchange protocol), services, technical architecture (nodes), building on the first step towards standardization that BMM constitutes;	Initiatives of standardisation exist in some communities (for instance IVEF for interfacing vessel traffic monitoring systems or basic ACO guidelines which contributes to flight safety during SAR operations) but the effort should be developed at both cross sector and EU level. (...) In order to ease information exchange and to propose a coherent framework to potential new partners, a data modelling effort should be encouraged. The aim is not to define the overall and complete data model, which could be time consuming and difficult to manage in the long term, but to agree on common definitions for core information and principles (e.g. technical standard). The modelling effort should focus on essential information to be exchanged during operational activities, especially cross sector.		Core
				Vision A
				Vision B
				Vision C
Regarding common services	Enhance and improve desirable core and common services, especially on security requirements (authentication, confidentiality, integrity, availability, traceability) and on enrichment of common services (alerts service, vessel of interest service, event common following service, etc.);	It is necessary to develop (and maintain) network of national contact points. Common framework could be created and within its limits information could be shared according to the single-window principle.		Core
				Vision A
				Vision B

	Recommendations coming from BlueMassMed	Recommendations coming from MARSUNO	Map to visions	
				Vision C

ANNEX 4 REQUIREMENTS COVERAGE IN DETAIL

The table below shows the detailed results of the requirements coverage exercise performed. Each Vision was tested against all principles and requirements. The notation used is the following:

- a complete fulfilment of a principle or requirement is indicated by a checkmark on a green background (✔). This gives the vision 1 point.
- a partial fulfilment of a principle or requirement is indicated by a dash (-) on a yellow background. This gives the vision 0, 3 points.
- a failure to fulfil a principle or requirement is indicated by a cross on a red background (✘). This does not give the vision any points.
- an unquantifiable fulfilment (at this stage) is indicated by a question mark on a grey background (?). This does not give the vision any points.

These scores allow calculating a weighted average for each of the visions, which is shown in the selection criteria in the vision template (refer to section 6 Architecture visions of CISE).

R or P		ID	Principle / Requirement	CISE Core	Vision A	Vision B	Vision C
Principles		P1	CISE must allow interlinking any public authority in the EU and in the EEA involved in maritime surveillance.	✔	✔	✔	✔
		P2	CISE must increase maritime awareness based on need-to-know and responsibility-to-share principles.	✔	✔	✔	✔
		P3	CISE must privilege a decentralised approach at EU-level.	✔	✔	✔	✔
		P4	CISE must allow interoperability among civilian and military information systems.	✔	✔	✔	✔
		P5	CISE must allow interoperability among information systems at the European, national, sectorial and regional level.	✔	✔	✔	✔
		P6	CISE must privilege reuse of existing tools and technologies.	✔	✔	✔	✔
		P7	CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance.	✔	✔	✔	✔
		P8	CISE must be system neutral.	✔	✔	✔	✔
		P9	CISE must make it possible for data providers to change their service offering	✔	✔	✔	✔
Requirements	Sharing	SI1	CISE must facilitate building and exchanging an integrated maritime awareness picture by authorities at national, sea basin, User Community or in the EU maritime domain level.	-	-	-	✔
		SI2	CISE must support sending information upon request, subscription or spontaneously.	✔	✔	✔	✔
		SI3	CISE must support sending notifications upon subscription or spontaneously.	-	✔	✔	✔
		SI4	CISE must support requesting information.	✔	✔	✔	✔

R or P		ID	Principle / Requirement	CISE Core	Vision A	Vision B	Vision C
		SI5	CISE must support subscribing and unsubscribing to information at any time.	✔	✔	✔	✔
		SI6	CISE must support subscribing and unsubscribing to notifications at any time.	–	✔	✔	✔
		SI7	CISE must support requesting or subscribing to information without knowing who the provider of the information is.	✘	–	–	✔
		SI8	CISE information requests can specify the time-frame for which the information is requested.	✔	✔	✔	✔
		SI9	CISE must rely on a common data model for information exchanges which is as language-neutral as possible.	✔	✔	✔	✔
		SI10	CISE must rely on a common transport protocol for information exchanges.	✔	✔	✔	✔
		SI11	CISE must rely on common standards for information processing.	✘	✔	✔	✔
		SI12	CISE participants must be able to approve information requests or subscriptions manually.	✔	✔	✔	✔
		SI13	CISE must support exchanges of large files.	✔	✔	✔	✔
		SI14	CISE participants providing information must provide statistics per service on information exchanged through CISE.	✔	✔	✔	✔
	Discovery	DI1	Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants.	✘	✔	✔	✔
	Discovery	DI2	CISE must allow retrieving contact information about CISE participants.	✔	✔	✔	✔
	Discovery	DI3	CISE must allow looking up what information CISE participants can provide and how they can provide that information.	✘	✔	✔	✔
	Discovery	DI4	CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate.	✔	✔	✔	✔
	Discovery	DI5	CISE must allow verifying if the services offered by CISE participants are available.	✔	✔	✔	✔
	Assurance	IA1	CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value.	✔	✔	✔	✔
	Assurance	IA2	CISE information requests must include an optional priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value.	✔	✔	✔	✔
	Assurance	IA3	CISE information exchanges must contain relevant characteristics about the information.	✔	✔	✔	✔
	Assurance	IA4	CISE participants must be able to acknowledge information received.	✔	✔	✔	✔
	Assurance	IA5	CISE participants must be able to provide feedback on the quality of the information received to the information provider.	✔	✔	✔	✔

R or P		ID	Principle / Requirement	CISE Core	Vision A	Vision B	Vision C
	Security	IS1	CISE information exchanges must respect agreed data access rights through access profiles.	✔	✔	✔	✔
		IS2	CISE must support information access rights that can be changed dynamically (respecting a commonly agreed SLA) by the information owner.	✔	✔	✔	✔
		IS3	CISE must support information providers providing a service to allow requesting access to their information.	✔	✔	✔	✔
		IS4	CISE information exchanges are authenticated at the level of the CISE participants and in respect of the CISE access profiles.	✔	✔	✔	✔
		IS5	CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret.	✔	✔	✔	✔
		IS6	CISE information requests and subscriptions can use different access profiles to request or subscribe to the same information.	✔	✔	✔	✔
		IS7	CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The transport protocol must also ensure higher levels of integrity depending on the classification level of the information.	✔	✔	✔	✔
		IS8	The communication channels between CISE participants must support non-repudiation.	✔	✔	✔	✔
		IS9	CISE must support interconnecting networks of different security levels, including public and private networks.	–	–	–	✔
	Collaboration	CO1	CISE must support secure exchange of unstructured information independent of the format the information is in.	✔	✔	✔	✔
		CO2	CISE participants should agree on a common set of file formats in order to maximise the usability of exchanged information.	✔	✔	✔	✔
		CO3	CISE must support secure audio communication.	✔	✔	✔	✔
		CO4	CISE must support secure video communication.	✔	✔	✔	✔
		CO5	CISE must support secure instant messaging.	✔	✔	✔	✔
		CO6	CISE must support secure white-boarding.	✔	✔	✔	✔
	Organisational	OA1	CISE must support an encompassing governance body that is required to maintain all the commonly agreed elements.	–	✔	✔	✔
		OA2	CISE participants should agree with availability and service levels defined in a bilateral, multilateral or community Service Level Agreement.	✔	✔	✔	✔

The table below summarises the scoring of each vision:

	Principles		Requirements		Total	
Vision	**∑**	**%**	**∑**	**%**	**∑**	**%**
CISE Core	9	100,00%	35,4	76,96%	44,4	80,73%
A	9	100,00%	42,5	92,39%	51,5	93,64%
B	9	100,00%	42,5	92,39%	51,5	93,64%
C	9	100,00%	46	100,00%	55	100,00%

ANNEX 5 HOW TO PROVIDE COMMENTS ON THIS DOCUMENT

As per CISE governance structure, all major deliverables produced in the context of CISE undergo a "Review Cycle", during which key stakeholders are invited to provide their comments.

Since the document authors needs to collect, compare and analyse the feedback from 28 Member States on the same document –potentially leading to a large number of comments – a tool is used that allows for easy extraction and aggregation of the comments from MS Word documents. In order for this tool to be able to capture all of your comments, please apply the following guidelines when commenting on this document:

- All comments are to be written in plain English. Comments provided in other languages cannot, unfortunately, be taken into account.
- The comments must be specific to and must relate to the text (sentence and/or paragraph) being revised.
- In case that you want to provide general comments or remarks that are not specific to a part of the text of this document, please provide them in a separate document and/or e-mail.
- Please use simple wording and be as specific, concise and clear as possible in order to avoid ambiguities.
- When referring to specific terms, acronyms or abbreviations that are common in your daily jargon, but that are not defined in the Glossary of this document, please define them first.

An MS Word comment is typically displayed as a red balloon in the right margin of the document and usually starts with the abbreviation of your name and the timestamp of when the comment was written. Depending on your version of MS Word, use the following steps for inserting a comment:

MS Word 2007 and MS Word 2010:

1. Write your comments directly in this MS Word document by first selecting a word, a part of a sentence or a paragraph (this can be done for example by double-clicking on a word or by dragging your mouse over parts of the text while keeping the left mouse button pressed).
2. Open the Review ribbon, select New Comment in the Comments section;
3. In the balloon that appears in the right margin, type your comment;
4. Click anywhere in the document to continue editing the document.

MS Word 2003:

1. Write your comments directly in this MS Word document by first selecting a word, a part of a sentence or a paragraph (this can be done for example by double-clicking on a word or by dragging your mouse over parts of the text while keeping the left mouse button pressed).
2. From the Insert menu, select Comment (or click on the New Comment button on the Reviewing toolbar);
3. In the balloon that appears in the right margin, type your comment;
4. Click anywhere in the document to continue editing the document.

The text will have coloured lines surrounding it, and a dotted coloured line will connect it to the comment. To delete a comment, simply right click on the balloon and select Delete Comment.

Attention:

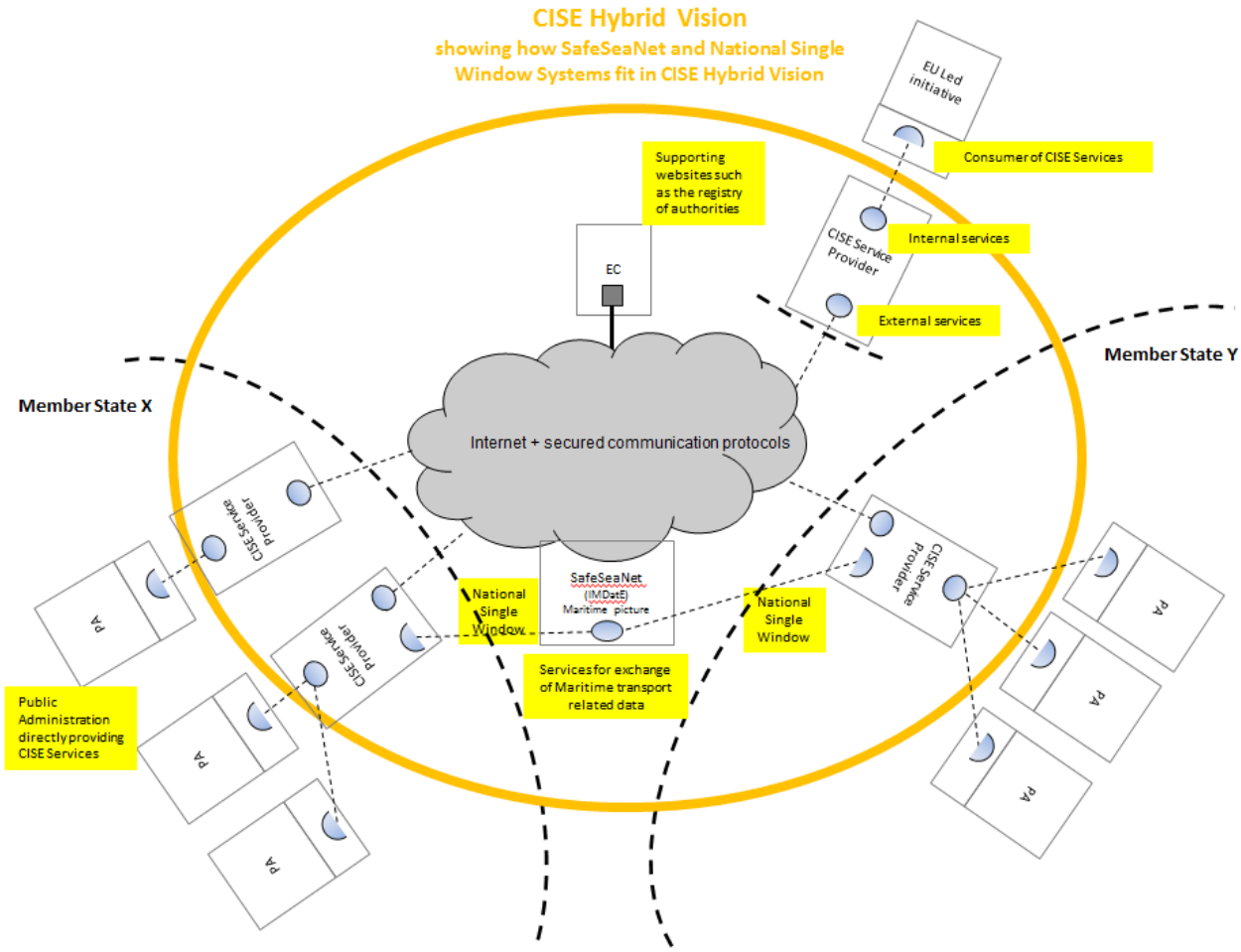
- Please note that a minimum of 4 characters must be selected in order for our commenting tool to grab the comment. Furthermore, comments on diagrams and embedded pictures are also not taken into account. In such cases, please select the caption text underneath the diagram or image.

- Please do not use the MS Word “track changes” tool and do not write your comments in the MS Word file.
- In case you need to translate this document to another language, and then translate your comments back to English, please make sure that your comments are provided in the form described above and that they have not been altered or moved to another section of the text during the translation process.
- If the comment is considered very important, please include the prefix 'MAJOR' in your comment.

ANNEX 6 FITTING EU INITITIATIVES IN THE HYBRID VISION

How do the Single National Window and SafeSeaNet fit in the hybrid vision?

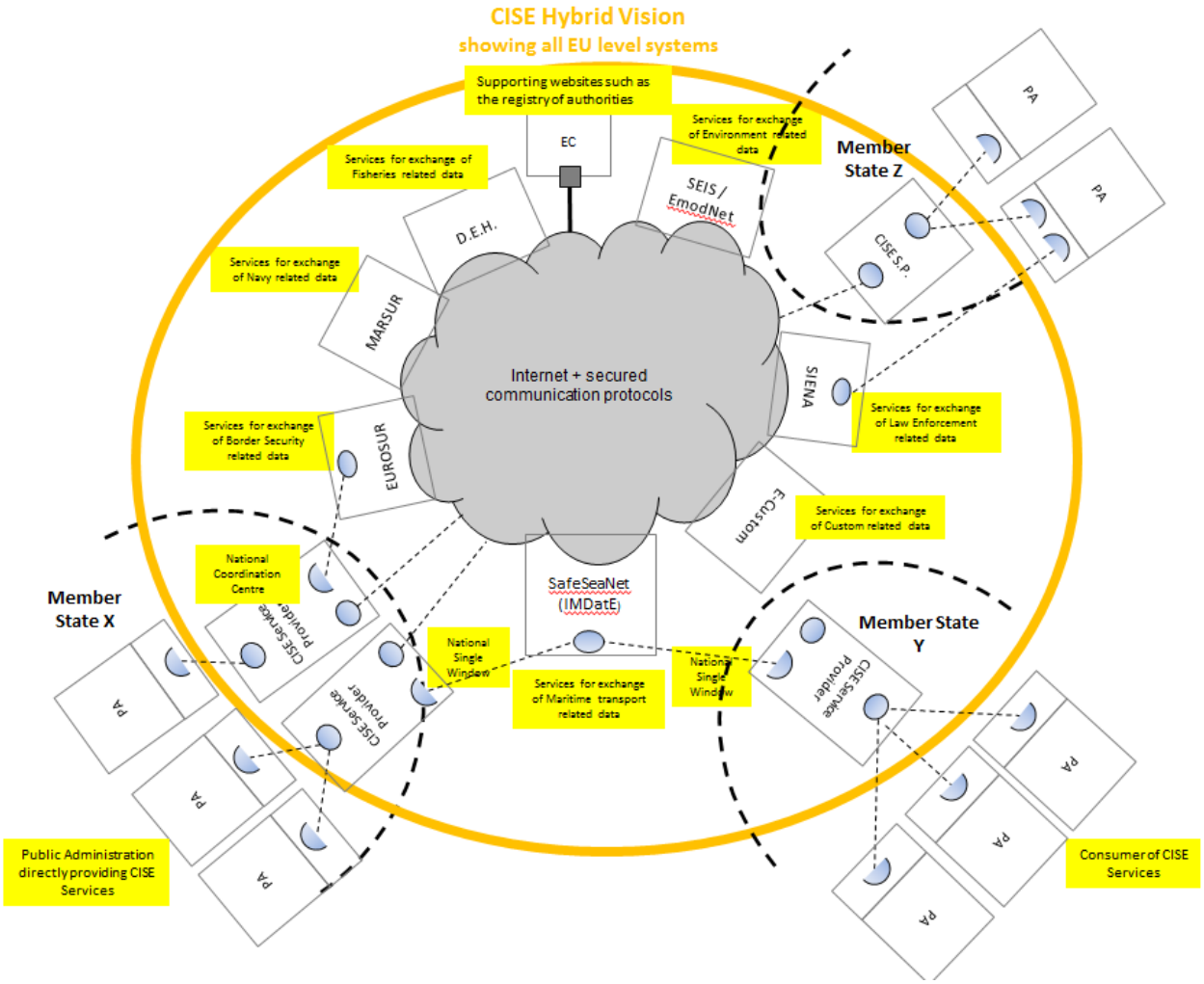
Several Member States have requested information about how the National Single Window projects to be carried out in the Member States, to implement Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports fit in the Architecture Visions document. A similar question was made about the systems operated by EMSA such as SafeSeaNet. The figure below shows how all these elements will fit together in CISE's hybrid vision.



In the hybrid vision, Member States may decide to expand their Single National Window to meet the requirements of the CISE Node. This is depicted in the figure above, where Member State Y decided to expand its National Single Window to meet the requirements of CISE. Member State X, on the other hand, decided to have multiple providers of CISE services. In this case, one of the two providers is the National Single Window of Member State X and the other one is a Public Administration participating directly in CISE with its own system supplemented with a CISE Node. The IMDatE system, which provides integrated information services based on SafeSeaNet, CleanSeaNet, Thetis and LRIT of EMSA will have a key role in CISE and will become a provider of CISE Services at EU level.

How do other European Initiatives fit in the hybrid vision?

The diagram below shows how all EU level systems and Member State systems can be connected through CISE.



It zooms into the technical details of the previous and highlights how each system has access to the shared environment. Access devices are necessary to ensure interoperability following the semantic and technical agreements reached in CISE Core.