Ref. Ares(2022)250279 - 13/01/2022

Practical Guide for joining the CISE network

Version 2.0
Date: 13 January 2022

Project funded
by the European Union

Table of Contents

List of Figures

List of Abbreviations

CISE	Common Information Sharing Environment
CINEA	European Climate, Infrastructure and Environment Executive Agency
CSG	CISE Stakeholder Group
DG MARE	European Commission's Directorate-General for Maritime Affairs and Fisheries
EEA	European Economic Area
EMFAF	European Maritime, Fisheries and Aquaculture Fund
EMSA	European Maritime Safety Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
EUMSS	European Union Maritime Security Strategy
EUROSUR	European Border Surveillance System Network
JRC	European Commission's Joint Research Centre
MARSUR	Maritime Surveillance Network
MS	Member States of the EU and EEA
RTS	Responsibility to share principle
SSN	Safe Sea Net
VMS	Vessel Monitoring System

Introduction

The purpose of the present guide is to provide an introduction to the Common Information Sharing Environment (hereafter CISE) to the maritime surveillance authorities in the EU/EEA interested in joining the network. Such authorities include public administrations from different maritime surveillance sectors from the Member States (MS), EU Agencies and other public bodies.

In addition to that, the present guide will also serve as an update on the developments of CISE to those already actively involved in the network. The content of this guide will be therefore further updated during the Transitional Phase of the project to reflect the progress made in CISE.

The guide is divided in 8 sections:

- **Section 1** is a short introduction to CISE including its background, key features, functionalities, as well as the composition and security standards of the CISE network.
- **Section 2**, **3**, **4** and **5** presents respectively the organisational, financial, technical, and operational aspects maritime surveillance authorities must consider when planning their connection to CISE.
- **Section 6** introduces the procured study for an audit on the implementation of the "responsibility to share" principle.
- **Section 7** presents CISE the communication tools and channels.

1. About CISE

1.1 Background

The Common Information Sharing Environment has the following political grounds:

- The progress made in the Transitional Phase coordinated by EMSA was recognized by the latest "**Council conclusions on maritime security**" adopted on 22 June 2021. In the conclusions, the Council also called for a widespread implementation of CISE as the interoperability solution in the EU maritime domain and encouraged further efforts to set up a fully operational network. Within this context, another important political result was achieved in June 2021, as the EUMSS Action Plan, which promotes the implementation of CISE, will be now monitored by a newly established Council preparatory body – the Working Party on Maritime Issues.
- Within the "**Council conclusions on a sustainable blue economy: health, knowledge, prosperity, social equity" on 26 May 2021,** the Council "encourages the Commission to continue its efforts to set up a fully operational Common Information Sharing Environment (CISE) for the maritime domain in cooperation with Member States and the relevant EU agencies".
- The "**Commission Communication on a new approach for a sustainable blue economy**" of 17 May 2021 highlights that a safe and secure maritime space is the prerequisite to preserving EU's strategic interests such as freedom of navigation, external border control or the supply of essential materials and for protecting economic activities and citizens, both at sea and on shore. The cooperation on coast guard functions between three key EU agencies generates significant economies of scale by reducing overlaps, developing multipurpose operations, and sharing aircrafts and vessels for search and rescuing operations, oil pollution response etc. The European Commission has developed a Common Information Sharing Environment for the maritime domain (CISE) to enhance information exchange. The Commission will propose rolling out the CISE's operational phase in 2024, subject to the results of the transition phase.
- **Council conclusions on Global Maritime Security** (19 June 2017 - 10238/17)

- **European Union Maritime Security Strategy** (EUMSS) – Action Plan adopted on 16 December 2014 and revised in 2018 - 17002/14

CISE key features:

- CISE for the EU maritime domain aims to make the existing Member State's (MS) maritime systems from seven different maritime sectors (maritime safety and security, marine environment, fisheries control, customs, border control, law enforcement, and defence) and the EU sectorial frameworks (SSN, VMS, EUROSUR, MARSUR, etc.) **interoperable to facilitate the exchange of unclassified and classified information** in a timely and efficient manner, while avoiding duplication.
- CISE has been designed **based on a voluntary collaborative process**, where sharing is not based on EU legislation but based on a spirit of cooperation.
- **CISE is not a (new) system or application** - it does not have a dedicated interface which implements specific use cases - but it is focused on providing cross-sectors and borders information system-to-system to top-up legacy systems. **CISE is a decentralized infrastructure, or network, based on nodes developed following a standard** (the CISE data and service model). In addition, CISE can be used in the future to share CLASSIFIED (EU-Restricted) information.
- The CISE's infrastructure has **two main building blocks**: i) a standard component that dispatches the information (so called CISE Node), and ii) the systems that an organization wants to connect to CISE (also called Legacy System) with its Adaptor. The Adaptor plays the crucial role to connect the organization's Legacy System to the node and at that level can decide which information should be consumed from and provided to the other participants connected to the network.
- **Data distribution policy** (including access rights) can be controlled and managed by a stakeholder at three levels: i) legacy system, based on its own access right management, ii) adaptor and iii) node. For what concerns the distribution policies that can be established at the node level it is important to mention that a stakeholder can define (among others): i) the authorities (called participants) that can receive the data, ii) geospatial and temporal conditions for the provision of information, and iii) the list of attributes to be shared.

CISE Transitional Phase:

- In 2019 based on the results of the EUCISE2020 project, COM (DG MARE) set up a preparatory action (hereafter called the "**Transitional Phase**") in preparation for possible implementation of CISE and its transition into operations. The Transitional Phase will last until December 2023.
- The main objective of the Transitional Phase is to turn the EUCISE2020 Research Project into a **European-wide operational network** open to all EU Member States and EU Agencies on a voluntary basis. This work entails to: establish conditions of use to regulate the sharing of information (called "Cooperation Agreement"); define an auditing scheme to foster the sharing capabilities among the stakeholders (based on the "Responsibility to Share" principle); establish an initial set of services to streamline the sharing of information in the operational phase; deliver a new version of the network to support the operational phase; and define the processes for exchanging CLASSIFIED information.
- In 2019 the **CISE Stakeholder Group**, to which "cross-sectorial" representatives of Member States and EU Agencies have been appointed, was created to manage the Transitional Phase of CISE. This group reports to the Member State Expert Sub-Group on the Integration of Maritime Security and Surveillance, and to the recently created by the Council conclusion the "Working Party on Maritime Issues".
- **EMSA** has been tasked with the setting-up and coordination of the Transitional Phase activities through two **Grant Agreements** with the European Commission (DG MARE) signed on 16 April 2019 and 26 November 2020 with a total budget of EUR 6.9 million (GA I: EUR 3.5 million and GA II: EUR 3.4 million). The CISE Transitional Phase started with the signature of the 1st GA, on 16 April 2019, and it will end on 16 December 2023.
- The **European Maritime, Fisheries and Aquaculture Fund** (EMFAF) offers a new funding opportunity to foster the implementation of CISE in the EU MS and to facilitate the engagement of new

stakeholders. The EMFAF supports a variety of activities including the implementation of the adaptor, hardware and the modernization of the legacy systems. In addition, the Commission has launched a call for proposals: “Action for a CISE incident alerting system”, with an available budget of EUR 2 437 500 to promote the development of information to be exchanged (see Section 3.2).

For further information about CISE, please refer to EMSA’s website for CISE: http://www.emsa.europa.eu/cise.html.

1.2 Functionality of CISE

An existing ICT system (hereafter called legacy system), owned by a stakeholder and used for maritime surveillance, can hold information that could be exchanged through CISE. The stakeholder uses an adaptor to translate the specific formats and communication protocols used by the legacy system to the CISE data and service model.

Through the CISE node, information can be shared with other CISE nodes in the CISE network. The CISE node is a common software for all the partners connected to the network, but the management is decentralized. The CISE decentralized architecture with a point-to-point exchange of information allows the stakeholders to be confident about data access and control.

In technical terms, the CISE Node is a common block ensuring the technical and semantic interoperability of CISE by managing the communication protocol among the Participants in the CISE Network.

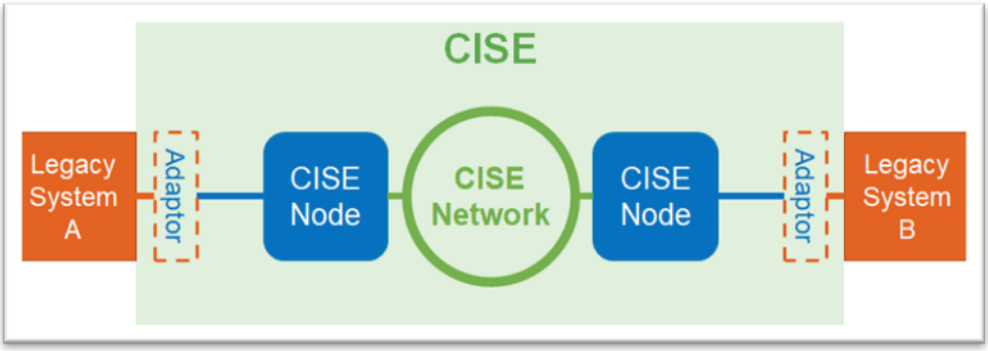

Figure 1. Main building block of the CISE hybrid architecture

To learn more, please see the Technical Specifications on EMSA’s website: http://www.emsa.europa.eu/technical-specifications.html.

1.3 The CISE network

The composition of the CISE network changes over time adding new nodes, legacy systems and data. A *Network diagram* providing the snapshot of the network composition can be found at the EMSA’s CISE website in the section CISE Network.

1.4 Security

The CISE network complies with the highest security standards and the network’s security is constantly monitored and improved.

The security plan is developed based on the EC Information Technology Security Risk Management Methodology and ISO 270001 practices.

The security by design and zero trust approach methodologies are used in CISE. Automated security testing tools are embedded in the system that can provide security reports both during the development and the operational phase of the CISE lifecycle.

1.5 CISE Welcome Package

All relevant information about CISE such as the CISE Transitional Phase Activities and Governance Structure, the technical specifications of the CISE building blocks (e.g., the CISE Node), and how to request support or training from EMSA/JRC can be found in the CISE Welcome Package.

The CISE Welcome Package is available in the collaborative space of the CISE Transitional Phase in Microsoft Teams (General > Welcome Package) and its content will be regularly updated by EMSA/JRC.

The CISE Welcome Package can also be requested by sending an email to the EMSA CISE team at mss@emsa.europa.eu.

2. Organisational aspects

2.1 Roles and responsibilities in the CISE network

When planning a connection to CISE, the concerned public authority is advised to identify from the very beginning the different roles needed for the running of CISE, the responsibilities attached to each role and the resources needed.

To this aim, a dedicated working group drafted the **CISE Cooperation Agreement** (CA)**,** which was approved by the CSG at the 6th CSG meeting on 9 and 10 February 2021.

Laying down the terms for the use of CISE and the rules for the information sharing in the CISE network, the Cooperation Agreement is the administrative basis and precondition for exchanging maritime surveillance information in a trusted network.

In this context, on 26 March 2021 the collection of signatures to the CA officially started following CISE secretariat's invitation to CSG members to sign the Agreement and fill in Appendix 1. All the public authorities from the Member States, EU Agency or relevant public body in the EU/EEA signing the Agreement will be referred as "**Party"** to the Agreement and hence will be obliged to comply with the stipulations and obligations contained in the Agreement itself.

Regarding the roles of the participants in the CISE network, these are defined in the Agreement as follows:

- "**CISE Node Owner**" or "**Node Owner**" is a Participant who is responsible for providing, managing, and maintaining a CISE Node. A CISE Node Owner must be Party to the Agreement.
- "**Participant**" stands for a public authority in a Member State or a body in the EU, responsible for maritime surveillance, that has a Legacy System connected to the CISE Network through a CISE Node. The Agreement also specifies that:
    - A Participant who is responsible for managing and maintaining a CISE Node is also a CISE Node Owner and a mandatory Party to the Agreement.
    - Public authorities or EU bodies not signing the Agreement but interested in exchanging information in the CISE Network can participate too only if they are represented by a Party to the Agreement.
- **"Other Party"** stands for any other public authority interested in joining the network and signing the Agreement which is neither a CISE Node Owner nor Participant.

To participate in the amendment process of the Agreement, each Member State or EU body must also appoint one Party – regardless of its role (Node Owner, Participant or Other Party) - which will be entitled to propose and vote on amendments to the Agreement. Such public authority is identified in the Agreement as "**Designated Party for amendments**".

The participants identified above must be listed in Appendix 1 to the Agreement that CSG members are invited to fill in and sent together with a signed full copy of the Agreement.

A copy of the Cooperation Agreement including Appendix 1 is available in the CISE Welcome Package subfolder in the CISE Transitional Phase collaborative space in Microsoft Teams. Frequently Asked Questions (FAQs) updated on a regular basis covering the main questions and answers regarding the Cooperation Agreement can also be found in the same subfolder.

A copy of the CA including Appendix 1 to fill in can also be requested by sending an email to the EMSA CISE team at mss@emsa.europa.eu.

Although outside of the remit of the Cooperation Agreement, the following function will need to be appointed:

- "**Node Administrator**" means the point of contact for the any issues regarding the daily operation of the Node.

All CSG members that have a node in place, must appoint a CISE Node Owner and a Node Administrator, who can be contacted, if needed.

2.2 Governance models

The CISE node and legacy systems can be set up following different governance models. The models presented in the table below should be seen as examples. Other examples are possible, and stakeholders are free to choose the model that best suits their individual needs.

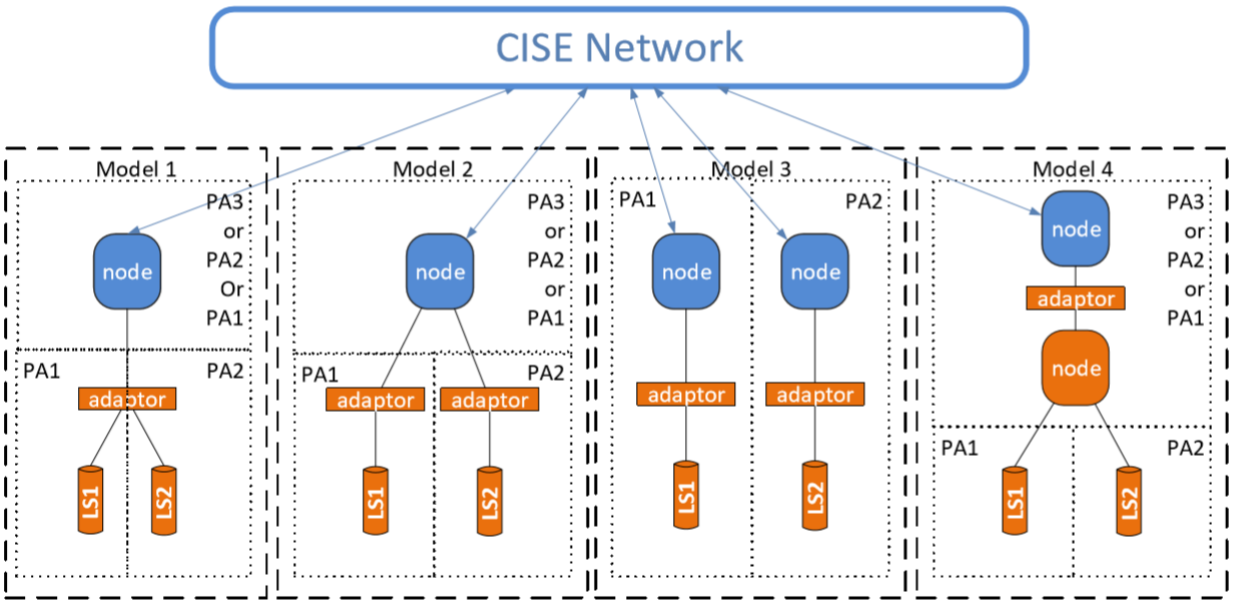

Figure 2. Examples of governance models

There is not one model that fits all participants and the model adopted will depend on national particularities and needs. These points should be considered before joining the network:

- Which legacy systems and authorities will be involved?
- How do authorities work at national level? Is there any coordinating authority?
- Is there already a central node orchestrating the information exchange in the country/EU Agency?

- Do authorities own one or several systems?
- What information will be shared or consumed?
- Where will the CISE node be hosted?
- Who will provide the resources to manage the CISE node? (declaration of new services, management of access rights etc.)

The following description of some models and their pros and cons can be useful for discussing the national set up.

2.2.1 Model 1: "One CISE node – one adaptor"

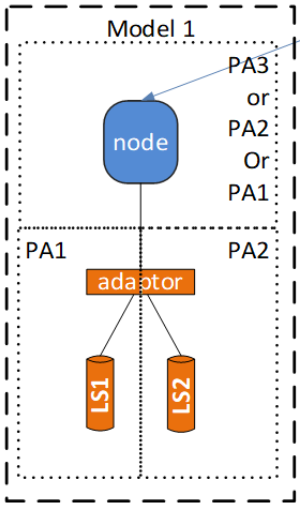

Figure 3. Model 1. "One CISE node – one adaptor"

In the CISE Governance Model 1, the different legacy system(s) is/are connected to the CISE node through one single adaptor.

+	▪ There is only a single adaptor to host and manage. ▪ The implementation of the adaptor is centralized, simplifying its management and procurement.
-	▪ The adaptor responsibility needs to be defined. ▪ The adaptor is more complex as it needs to support different models and protocols and has to deal with the redistribution of information in case of different legacy systems connected. ▪ Interfaces in the legacy system shall be coordinated with the authority in charge to manage the adaptor in order to guarantee the business continuity.
This model is recommended where the number of the authorities that need to connect their legacy system with the node is limited (2 or 3) and there is already a coordination among them at the national level. This is also recommended in case of the connection to CISE of a national system already gathering and fusing maritime information.	

2.2.2 Model 2: “One CISE node – more than one adaptor”

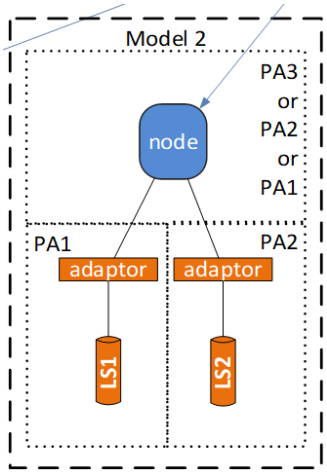

Figure 4. Model 2. “One CISE node – more than one adaptor”

In the CISE Governance Model 2, the different legacy systems are connected to the CISE node through their respective adaptor.

+	The adaptor responsibility is easier to target when it relates to one legacy system only.
-	Each authority that wants to connect to the legacy systems has to procure its own adaptor.
This model is recommended where the number of the authorities that need to connect their legacy system can be high and there is not a pre-defined coordination among them at the national level.	

2.2.3 Model 3: “One country with more than one CISE node”

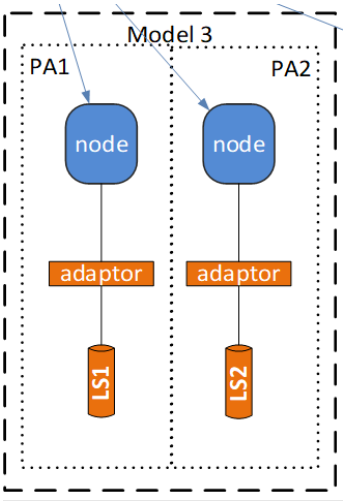

Figure 5. Model 3. “One country with more than one CISE node”

Governance Model 3 can be suitable for a country having two separate nodes, governed by two different public authorities. The figure displayed above should be seen as an example. More than one Legacy System can be linked to each adaptor, for instance.

+	▪ This solution could simplify the decision at the national level about the authority in charge of the node. ▪ The adaptor responsibility is easier to target when it relates to one legacy system only.
-	The separated governance and dissemination of data also creates costs related to the management of the nodes.
This model is recommended when authorities in the MS want to keep a quite high independent governance either in terms of strategy to join to CISE or in the information to share.	

2.2.4 Model 4: "National node connected to the CISE node"

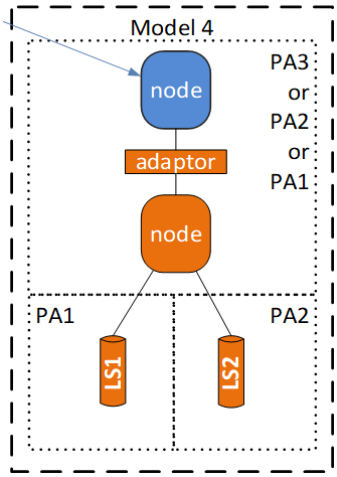

Figure 6. Model 4. "National node connected to the CISE node"

Governance Model 4 can fit a MS that will have its national legacy systems connected to a national node (i.e. an IT system that redirect messages or may consolidate the information in its own database), which in turn connects all the national authorities to the CISE node.

+	▪ This solution permits making use of the CISE building blocks to enable interoperability between authorities at the national level and national operational solution. ▪ National nodes could apply their own access control procedures in addition to the CISE node.
-	▪ In this model one of the challenges is to decide who is the authority in charge to manage the node at national level including the procurement of the operational support and the implementation and maintenance of the adaptors. ▪ This kind of model might be the most challenging in terms of access control. If only one common adaptor (and only one certificate) is used, then the CISE network will authenticate the national node as CISE Participant and CISE access right rules will be set for the national node, not for the legacy systems behind it.
This model is recommended for MS that needs to target interoperability also at the national level.	

3. Financial aspects

3.1 Costs

How much does it cost to connect to the CISE network? Costs may vary from stakeholder to stakeholder as they depend on:

- Public procurement costs.
- Type of CISE services to develop.
- The governance model chosen (see section 2.2).

More specifically, there are three cost macro-categories that maritime surveillance authorities interested in connecting to the CISE network must consider. These three cost categories are: the infrastructure, the software, and the personnel. In addition to these, the costs related to the provisioning of the CISE services must be also taken into account.

3.1.1 The infrastructure

To be able to connect to the CISE network, the infrastructure needed includes:

- The **network equipment**, namely the router for the VPN to create and manage 30 connections approximately.
- The **hardware for the CISE node**, whose standard configuration might have a variable cost of approximately 10-15K EUR.
- The **hardware for the adaptor**, whose cost varies depending on the systems connected and the information shared.

3.1.2 The software

The second cost category to consider relates to the software of the node and the adaptor. More specifically, in terms of costs, stakeholders must consider the following:

- **Node software**. Stakeholders are free of charge for this cost. The Commission, through EMSA and JRC, is in charge to develop, maintain and provide operational support for the node software to the stakeholders.
- **Adaptor software**. The cost needs to be estimated case by case. It largely depends on the capabilities of the legacy systems and the number of CISE services to be developed. In the case of the *pilot adaptor*, the development of the software is provided for free by the Commission (JRC) to stakeholders.

3.1.3 Personnel

The third cost category to consider relates to the personnel essential to the implementation of CISE. The personnel include the:

- **Node Administrator,** in charge of the management of the node, of the configuration and maintenance of the router for the VPN and the connection between the router and the server, as well as of the security protocols.
- **Maritime Centre Operator,** responsible for managing and processing the information exchanged at the operational centre.

None of the two responsibilities is a full-time job.

3.1.4 Technical and Operational support for the adaptor

To guarantee the provisioning of the CISE services during the transitional phase, technical and operational support for the adaptor should be put in place by the stakeholders. Technical support will be needed for the evolutive maintenance of the adaptor (i.e. new functionalities, request for changes and fixing bugs) while operational support for the incidents and problem investigation.

If needed, the CISE technical team can be consulted in the preparation of the procurement documentation to set up the technical specifications for the implementation of the adaptor.

3.2 Funding opportunities

As mentioned in the previous section, the software of the node including the development, the evolutive maintenance, the technical and operational support, is offered **at no charge** by the Commission (EMSA and JRC) to the stakeholders.

Therefore, the stakeholders are in charge of:

- Procuring the infrastructure of the node and the adaptor including the network equipment.
- Procuring the software of the adaptor and its evolutive maintenance.
- Covering personnel costs as specified in section 3.1.3.

Such activities are supposedly at the expenses of the stakeholders. However, the Commission through the European Maritime, Fisheries and Aquaculture Fund (EMFAF) that entered into force on 14 July 2021 and is running from 2021 to 2027 provides financial support to stakeholders to cover such expenses and support them in implementing CISE.

3.2.1 How can the EMFAF financially support the implementation of CISE?

With a total available budget of €6.108 billion, the EMFA fund is divided between the “shared management” and “direct management”, offering stakeholders two different funding channels to co-finance their CISE-related activities.

- Shared management

  Under the “shared management”, €5.311 billion is provided to the Member States[1] which are called upon to draft and submit to the Commission their national programme for observation and approval. More concretely, each Member State is invited to present its public investment plan covering the EMFAF programming period (2021-2027) and its planned actions to fulfil the objectives of the fund and meet the fund´s priorities.

  Under Priority 4, namely “*strengthening international ocean governance and enabling seas and oceans to be safe, secure, clean and sustainably managed*”, which also fosters maritime surveillance under CISE, the fund can be used during the entire programming period to co-finance the expenses linked to:

  - the technical setting up of CISE in terms of infrastructure and software.
  - staff costs which are fully within the scope of the CISE-related operations and essential to its implementation.

[1] National allocations are established on the basis of the 2014-2020 shares under under Regulation (EU) No 508/2014 of the European Parliament and of the Council on the European Maritime and Fisheries Fund (the ‘EMFF’).

Each Member State must designate the public administration that will be responsible to submit and coordinate the fund at the national level (national contact point). The CISE stakeholders must therefore make sure that their needs are expressed to that administration in order to use the fund to co-finance their CISE-related activities

The template of the 2021-2027 EMFAF national programme can be found here.

- Direct management

Under the "direct management", the amount of €797 million was allocated in the framework of the EMFAF. Such funding is directly managed by the Commission through work programmes by awarding grants (via call for proposals) and procurement contracts (via call for tenders).

In the context of CISE, the first call for proposal "Action for a CISE incident alerting system" was launched on 26 August 2021 by the European Climate, Infrastructure and Environment Executive Agency (CINEA) with the aim to co-finance one single project to enhance the cooperation between public maritime authorities by promoting the development of at least 2 services at pre-operational phase and to foster the uptake of CISE in view of its operationalisation.

More information on future Calls for proposals under the EMFAF can be found on CINEA website here.

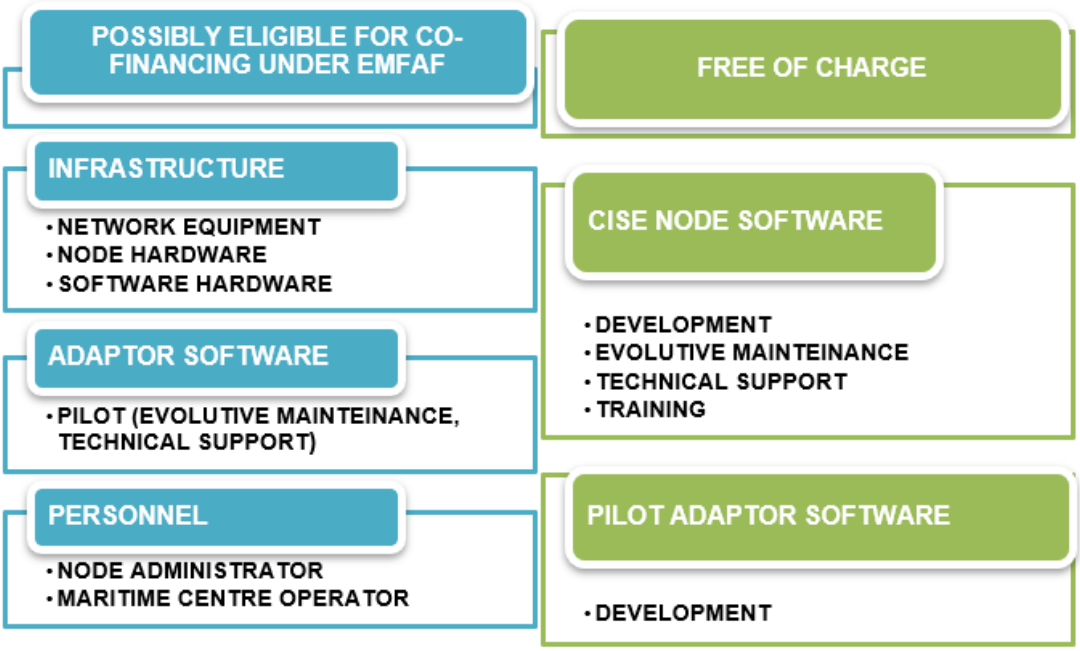

Figure 7. CISE costs and EMFAF financial support

4. Technical aspects

4.1 Technical documentation

The CISE Technical Specifications can be found at the CISE website: http://www.emsa.europa.eu/technical-specifications.html.

4.2 CISE Support Team

To support the activities of the CISE stakeholders during the Transitional Phase, EMSA and JRC have established a pre-operational organisation and several support processes:

- incident and problem management.
- node configuration.
- node maintenance.
- node deployment.
- adaptor development.
- conformity testing.

Technical and operational support is provided by the CISE Support Team which is organised at 3 levels:

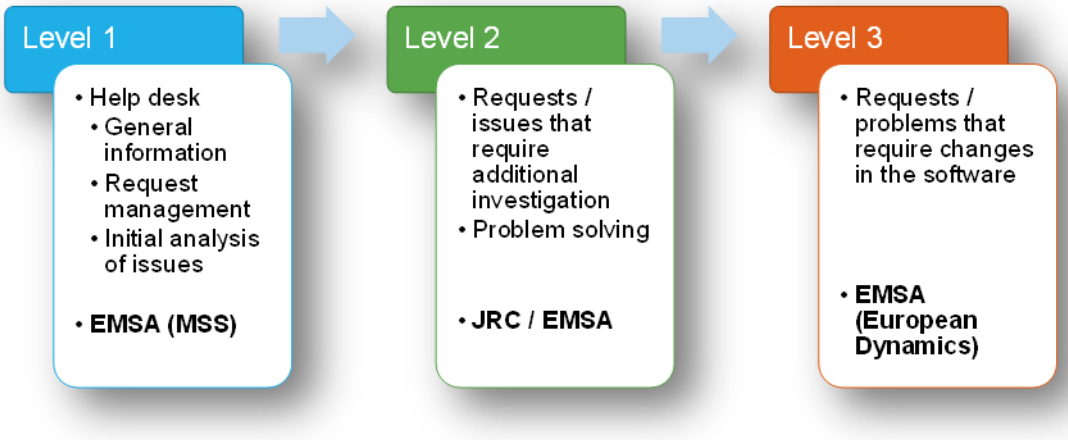

Figure 8. Support levels

For further information about the support, please refer to the Technical and Operational Support document on the CISE website in the Technical Specifications section.

4.3 Standardisation

The formalisation of the CISE standards, i.e., the CISE Data model and the CISE Service model, is under discussion in the Industry Specification Group (ISG) “European Common Information Sharing Environment Service and Data Model (CDM)” in ETSI (European Telecommunications Standards Institute).

More information about the group can be found on the ETSI website.

5. Operational aspects

5.1 Information shared

When planning the connection to the CISE network, it is crucial to decide which information will be shared: provided and consumed. CISE is a voluntary network, which builds on the contribution from its participants. It is therefore of utmost importance that the MS or EU Agency asks itself not only which information or services it wants to receive through CISE, but also what information or services it has available to share that can be valuable to the other CISE participants.

This proactive information sharing attitude enables the further distribution of the information within the CISE community, even when not specifically requested by another party, reaching any public authority that may

have a legitimate use of it. An access rights template defined for each provider and embedded into their node, establishes the access limits to the information.

Based on the business needs of each organization, CISE participants are requested to define the information services that they want to provide and to consume (see the CISE data and service model: http://emsa.europa.eu/technical-specifications.html). A Catalogue of services deployed in the network in their most updated version can be found in the collaborative platform (Microsoft Teams) in CISE Stakeholders Group channel. The Catalogue is updated and distributed to the CSG after each CSG meeting. Participants are encouraged to add services to these lists and keep EMSA updated on any planned changes.

5.2 Pre-operational services

There is an on-going activity to review and identify the services with more operational added value in order to implement them into a pre-operational network, on which basis the operational phase of CISE will be built.

This work is meant to address not only the technical aspects (i.e. technical support or testing exercises) but also operational (i.e. drafting of operational procedures). From an operational point of view, the management of the pre-operational services in each Maritime Awareness Centre will require the adaptation of their current Standard Operating Procedures or the drafting of new ones. To support such work the Operational working group has been established, where representatives from stakeholders are appointed.

During the Transitional Phase, some operational exerCISEs will be organized to declare the operational capability of the network.

5.2.1 Operational exerCISEs

The aim of these exercises is to support the establishment of the identified pre-operational services during the Transitional Phase to achieve the initial operational capability of the network.

These exercises are based on the execution of representative use cases by using the implemented pre-operational services among operators from different maritime centres.

5.3 Training and best practices

One of the activities under the Transitional Phase is to define the training needs and to facilitate the sharing of best practices and lessons learnt amongst the CISE Stakeholders. To enable the sharing of knowledge, EMSA organises regularly training courses and themed workshops. During the project, online training modules will be developed.

Since the beginning of the CISE Transitional Phase in 2019, 4 workshops (see Figure 9) and 4 training courses (see Figure 10) have been organised.

CISE Workshops	Best Practices Workshop	11 December 2019
	Workshop on pre-operational services	02 December 2020
	Workshop for the Baltic Sea region	28 April 2021
	EMFAF Workshop	30 September 2021

Figure 9. CISE Workshops

As to the training courses organised by EMSA, the first one was a two-day course for Node Administrators which took place in July 2020. The topics addressed included an introduction to the CISE node architecture, management of the node and management of the services. In addition to the technical materials shared, this exercise served to connect node administrators from different stakeholders and to build a network through which best practices and problem-solving approaches could be shared.

CISE Training courses	1st Node Admin Training	1 & 2 July 2020

2nd Node Admin Training	24 & 25 November 2020
Introduction to CISE Training	16 June 2021
3rd Node Admin Training	14 October 2021

Figure 10. CISE Training courses

CISE stakeholders are encouraged to share their knowledge and to consider whether nationally arranged training activities can be opened to stakeholders from other organisations and countries. If feasible, EMSA can assist in dissemination of information.

6. Responsibility to share

One of the activities outlined in the CISE Transitional Phase is to conduct a study for an audit on the implementation of the "responsibility to share" principle. The "responsibility to share" principle (RTS) is based on the idea that stakeholders take the responsibility to voluntarily share any information they deem useful for any one or more stakeholders of the CISE network.

A proactive information sharing attitude is key to CISE as it will enable the further distribution of the information within the CISE community. Ideally this should occur even when the information has not been specifically requested by another party and reaching any authority that has legitimate use for it. As a result, the overall performance of the European authorities responsible for maritime surveillance will improve.

In order to promote the RTS principle, the ongoing exchange of information of the network will be captured through voluntary audits. These will provide "pictures" of what information is being shared and provide framework to see what else could potentially be shared in the future.

In this context, a study has been procured to define a methodology to support MS to implement the RTS by identifying weaknesses and gaps and proposing suitable measures for mitigation and improvement. The main aim of the study is to help to define the possible criteria for measuring and promoting the sharing of information within the CISE network.

In 2020 the RTS Working Group was set up, with nominated members from the Member States, to support and advise on the design of this study.

7. Communication

EMSA has arranged a number of communication channels for the CSG. The choice of tool will depend on the purpose of the information sharing and will supplement each other.

A dedicated section for CISE is set up on EMSA's website: www.emsa.europa.eu/cise.html. It will serve as the main content and navigation hub for online visitors.

The collaborative platform, set up in Microsoft Teams, is the restricted area to be used by the members of the CSG, its working groups and other invited users only.

EMSA has established a single point of contact for any technical and administrative requests or questions related to CISE. To get in contact with the CISE Team at EMSA please write at mss@emsa.europa.eu.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu