Practical Guide for joining the CISE network

Version 4.0 – 30 May 2025

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 Stakeholders 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
ISP	Information Sharing Plan
LS	Legacy System
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**") for maritime surveillance authorities in the EU/EEA interested in joining the network. Such authorities include public administrations from different maritime surveillance sectors from the EU Member States, EEA member countries and EU Agencies.

In addition to that, the present guide will also serve as an update on the developments of CISE for those authorities / members that already actively involved in the network. The content of this guide will be subject to periodic updates in order to ensure its accuracy and relevance.

The guide is divided into 7 sections:

- **Section 1** provides an introduction to CISE including the political background, CISE key features as well as the composition and security standards of the CISE network.
- **Sections 2**, **3**, **4** and **5** present respectively the organisational, financial, technical, and operational aspects maritime surveillance authorities and interested EU Agencies should consider when planning their connection to CISE.
- **Section 6** introduces the "Responsibility to Share" principle.
- **Section 7** presents the CISE communication tools and channels.

1. About CISE

1.1 Political background

The Common Information Sharing Environment has the following political grounds:

- The **Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan** adopted on 24 October 2023, highlights the key role of CISE, which will "facilitate real-time information sharing between different authorities responsible for coast guard functions, including the military, connecting concerned authorities within and across Member States".
- The **Strategic Compass for Security and Defence**, adopted on 21 March 2022, underlined that, on the basis of an updated EU Maritime Security Strategy (EUMSS), the EU will further develop and strengthen the EU's maritime security awareness mechanisms such as CISE to advance interoperability, facilitate decision-making and support increased operational effectiveness.
- The progress made in developing CISE was recognized by the "**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, it is important to mention that as of June 2021 the EUMSS Action Plan, which promotes the implementation of CISE, is monitored by a Council preparatory body – the Working Party on Maritime Issues.
- Within the "**Council conclusions on a sustainable blue economy: health, knowledge, prosperity, social equity"** adopted 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 the Member States and the relevant EU agencies".
- **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
- **Council conclusions on integration of Maritime Surveillance** (23 May 2011, 3092nd GENERAL AFFAIRS Council meeting)

1.2 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 is designed **as a voluntary collaborative process**, where information exchange is based on a spirit of cooperation and is not enforced by legislation.
- **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-sector and cross-border information system-to-system to top-up the existing legacy systems (LS). **CISE is a decentralized infrastructure, or network, based on nodes developed following a standard** (the CISE data and service model). In addition, in the near future, CISE will be able to be used to share CLASSIFIED (EU-Restricted) information.
- The CISE's infrastructure has **two main building blocks**: i) a standard component that dispatches the information (the so called CISE Node), and ii) the systems that an authority wants to connect to CISE (i.e., legacy systems) with its Adaptor. The Adaptor plays the crucial role of connecting an authority's legacy system to the node, and at that level an authority 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.

1.3 CISE Transitional and Operational Phases

In 2019, based on the results of the EUCISE2020 Research project, the Commission (DG MARE) set up a preparatory action (hereafter called the "**Transitional Phase**") to last until June 2024 with the main aim of turning the EUCISE2020 project into a European-wide operational network open to all EU Member States and EU Agencies on a voluntary basis.

The main objectives of the Transitional Phase were successfully met: the conditions of use to regulate the sharing of information was established by setting up the so-called "Cooperation Agreement"; the methodology to foster the sharing capabilities among the stakeholders (based on the "Responsibility to Share" principle) was defined; an initial set of operational services to streamline the sharing of information in the operational phase were elaborated; a new version of the network to support the operational phase was delivered; and the processes for exchanging CLASSIFIED information were defined.

Based on the outcomes of the CISE Transitional Phase (2019-2023), the Commission (DG MARE) set up the **Operational Phase** of CISE with the aim of becoming fully implemented in the operational activities of maritime surveillance authorities. The Operational Phase started on 1 July 2024.

1.4 Functionality of CISE

An existing ICT system (hereafter called "legacy system"), owned by authorities and used for maritime surveillance, can hold information that could be exchanged through CISE. To enable the exchange of such information amongst different authorities, CISE offers the following standard building blocks:

- The **CISE Node**, which is a common software for all the maritime authorities connected to the network and allows them to provide and consume the information available in the network. The decentralized architecture of the CISE Node allows the authorities to be confident about data access and control over the information shared. 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.

- The **adaptor** connects the authorities' maritime surveillance systems (i.e., legacy systems) to the node. In technical terms, the **adaptor** translates the specific formats and communication protocols used by the legacy system to the CISE data and service model (and vice versa).

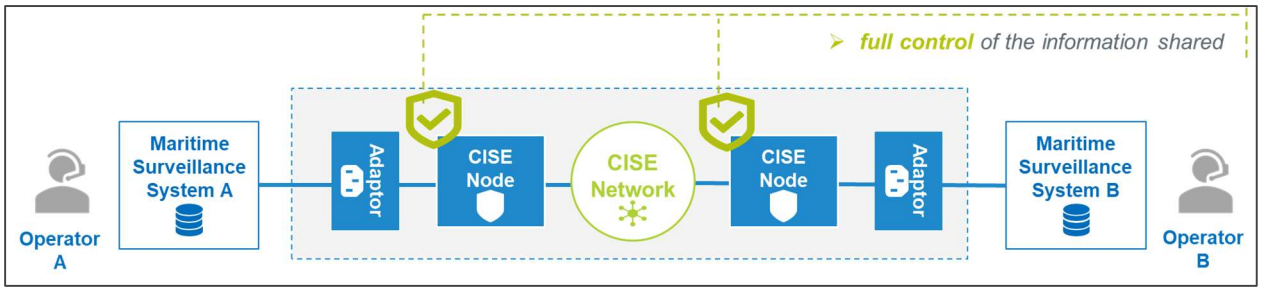


Figure 1. Main building blocks of the CISE decentralized architecture

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

1.5 Information shared in the CISE network

CISE enables the sharing of all types of maritime information, also information used both by the civil and military organisations. The actual information exchanged depends on what information CISE participants will offer.

Currently, it is possible to share **unclassified information**. However, in the first stage of the Operational Phase, there is an ongoing activity to develop the initial operational capabilities with a limited number of authorities able to exchange **classified information** through CISE by the end of 2026. The CISE Classified Network will be able to handle classified information up to "EU Restricted" and will be used to connect participant's "Classified ICT systems".

CISE participants will be able to be part of both the unclassified and the classified network on a voluntary basis.

1.6 Security

The CISE security approach is based on the European Commissions' IT Security Risk Management Methodology (ITSRM) to evaluate the security controls needed to be implemented in order to achieve the appropriate security level. The CISE network has adopted the security by design and zero-trust approach methodologies. 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. The network's security is constantly monitored and improved. Based on the risk assessment and the CISE security plan, the security posture of the network is constantly evaluated, and new security controls are introduced when needed. Security and penetration tests are performed before every new release to verify that all known vulnerabilities have been addressed and mitigated.

A set of information security guidelines are being developed for CISE, that all the CISE participants will agree upon and be aware of. This will enable them to evaluate their current security status against these guidelines, communicate that information to the other CISE stakeholders and examine how any existing gaps can be closed. In that way, the necessary trust and decisions for exchanging information using CISE will be built on concrete evidence for the security status of all CISE participants. These guidelines are based on the recommendations covering all relevant parts of the Commission Decision C(2017)46 of 10 January 2017, concerning the security of information systems used by the European Commission, international standards and IT Security good practices and follow ISO 27001.

1.7 CISE Welcome Package

The CISE Welcome Package includes all relevant information about CISE such as the Operational Phase activities and governance structure, the technical specifications of the CISE building blocks (CISE Node and adaptors), and how to request support or training from EMSA.

CISE stakeholders can request access to it by sending an email to the CISE Support 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 authority is advised to identify from the very beginning the different roles needed for the running of CISE, the corresponding responsibilities, and the resources needed.

To this aim, a dedicated working group composed of experts nominated by the EU MS and EU Agencies drafted the **CISE Cooperation Agreement** (hereafter "CA"), which was approved by the CISE Stakeholders Group at the 6th CSG meeting held on the 9 and 10 February 2021.

The Cooperation Agreement regulates the information sharing within the CISE network. By signing the Cooperation Agreement, authorities commit themselves to putting in place processes that guarantee that the information shared is accurate, reliable, secure and protected (by safeguarding confidentiality, data security and data ownership).

The Cooperation Agreement does NOT impose which data an authority has to share. Each authority is free to decide which data it intends to provide to the network (this information is declared in the Information Sharing Plan).

In this context, in March 2021 the collection of signatures of the CA from the CISE stakeholders officially started.

In line with the terminology used in the CA, any EU MS public authority, EU Agency or relevant public body in the EU/EEA signing the Agreement is referred to as a "**Party"** to the Agreement. By signing, each Party will have to comply with all the stipulations and obligations contained in the Agreement.

With regard to the roles of the MS authorities/EU Agencies participating 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 setting up, managing and maintaining a CISE Node. A CISE Node Owner must be a Party to the Agreement, meaning therefore that Node Owners have the obligation to sign 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 Agencies not signing the Agreement but interested in exchanging information in the CISE Network can participate too but only if they are represented by a Party to the Agreement.
- **"Other Party"** stands for any other public authority or body in the EU interested in joining the network which signs the Agreement being neither a CISE Node Owner nor a Participant.

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

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

A copy of the Cooperation Agreement including Appendix 1 can be requested by sending an email to the EMSA CISE team at mss@emsa.europa.eu. The Frequently Asked Questions (FAQs), updated on a regular basis and covering the main questions regarding the Cooperation Agreement, will also be sent together with the copy of the Agreement.

Although outside of the remit of the Cooperation Agreement, the following function will also need to be appointed when planning a connection to CISE:

- "**Node Administrator**" who will act as the point of contact for 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 (LS) 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.

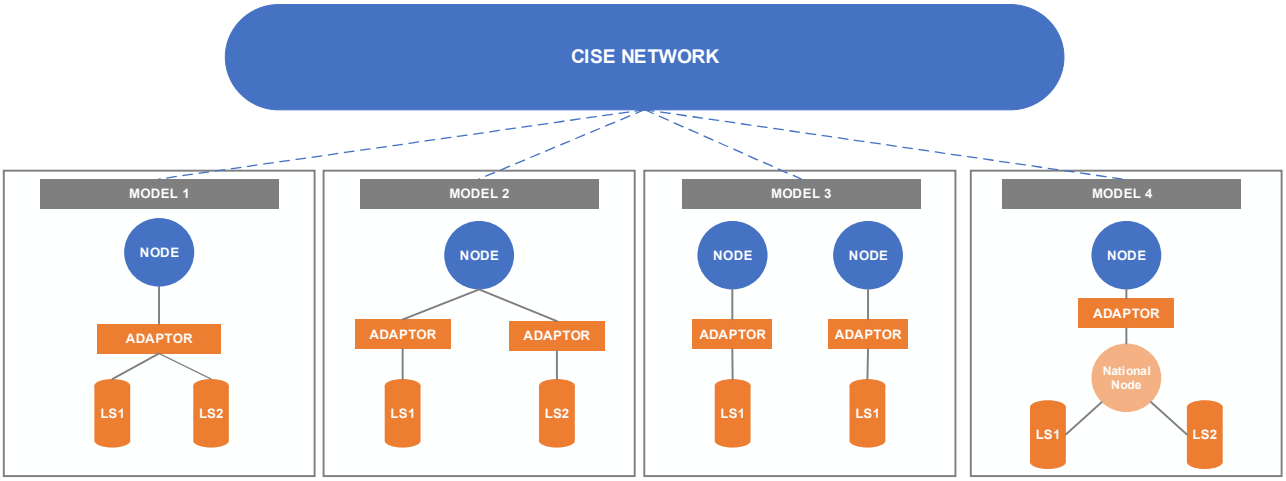


Figure 2. Examples of governance models

There is not one model that suits 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? (implementation 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”

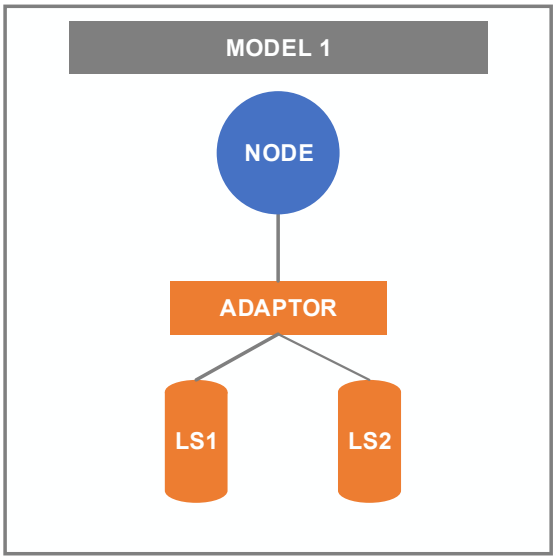


Figure 3. Model 1. “One CISE node – one adaptor”

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

Pros	▪ There is only a single adaptor to host and manage. ▪ The implementation of the adaptor is centralized, simplifying its management and procurement.
Cons	▪ 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 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 coordination among them at national level. This is also recommended in case the connection to CISE of a national system is already gathering and fusing maritime information.	

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

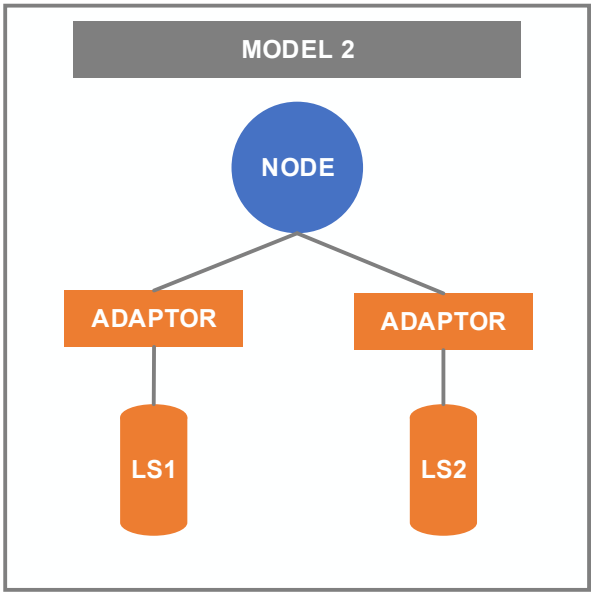


Figure 4. Model 2. “One CISE node – more than one adaptor”

In the CISE Governance Model 2, the different legacy systems are connected to the CISE node through their respective adaptors as shown in the figure above.

Pros	The responsibility for the adaptor is easier to be defined when it relates to one legacy system only.
Cons	Each authority needs to procure their own adaptor to connect their legacy systems.
This model is recommended where the number of the authorities that need to connect their legacy systems is high and there is no pre-defined coordination among them at national level.	

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

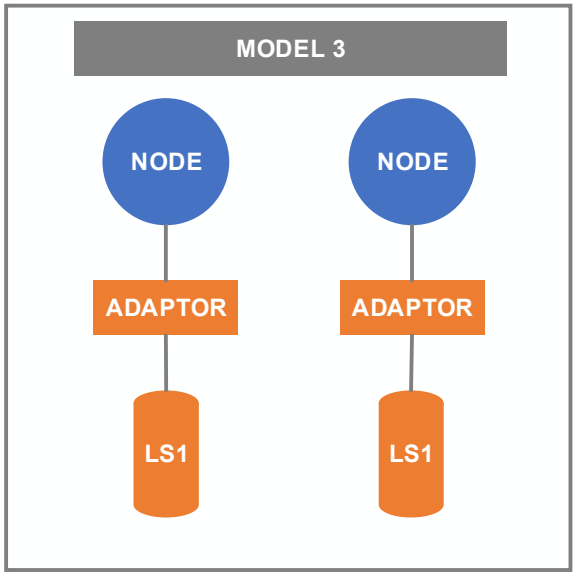


Figure 5. Model 3. “One country with more than one CISE node”

In the CISE Governance Model 3, there are two separate nodes, governed by two different public authorities each connected to their own adaptor as shown in the figure above.

Pros	▪ This solution could simplify the decision at the national level about the authority in charge of the node. ▪ The responsibility for the adaptor is easier to be defined when it relates to one legacy system only.
Cons	The separated governance and dissemination of data creates costs related to the management of the nodes.
This model is recommended when authorities in the same MS want to keep a high level of independency both in terms of strategy to join CISE and in deciding on the information to be shared.	

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

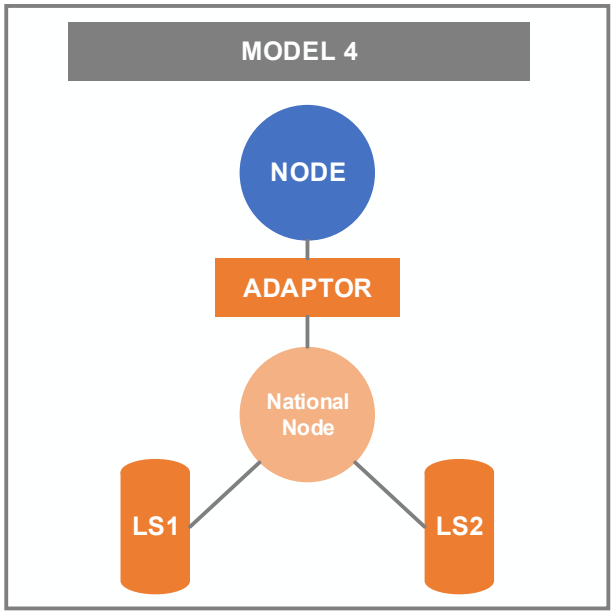


Figure 6. Model 4. "National node connected to the CISE node"

In the CISE Governance Model 4, national legacy systems are 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 as shown in the figure above.

Pros	▪ This solution permits using the CISE building blocks to enable interoperability between authorities at the national level. ▪ National nodes can apply a specific access control matrix at national level in addition to the CISE node's.
Cons	▪ In this model, one of the challenges is to decide who is the authority in charge of managing the node at national level, including the procurement of the operational support and the implementation and maintenance of the adaptor. ▪ 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 need 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 information exchange services to be developed;
- The governance model chosen (see section 2.2).

More specifically, there are three macro cost categories that maritime surveillance authorities interested in connecting to the CISE network must consider. These three cost categories are:

1. **Infrastructure**;
2. **Software**;
3. **Personnel**.

In addition to these, the costs related to the Legacy Systems (e.g., new functionalities to share/use information, maintenance, etc.) must also be considered.

3.1.1 Infrastructure

To be able to connect to the CISE network, the stakeholders would need the following elements:

- 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 for the on-premises installation. The cost on cloud installation may vary due to contractual matters.
- The **hardware for the adaptor**, whose cost varies depending on the systems connected and the information shared.

3.1.2 Software

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

- **Node software**. The node software is free of charge. The Commission, through EMSA, is in charge of developing, maintaining and providing 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 information exchange services to be developed.

3.1.3 Personnel

The third cost category to be considered relates to the personnel essential for the implementation of CISE. The personnel includes the:

- **Node Owner** - responsible for the CISE node, including the implementation of the Information Sharing Plan (ISP), the overseeing of incidents in the node, the definition of the access rights, the availability of the node.
- **Node Administrator** - in charge of the technical 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 a maritime operations centre.

None of these roles constitutes a full-time job.

3.1.4 Technical and Operational support for the adaptor

To guarantee the provisioning of the CISE services, the stakeholders should provide/procure technical and operational support services for the adaptor including: 1) software development services for the adaptor (i.e., development of new functionalities, request for changes and fixing bugs) and 2) operational support (i.e., incidents and problem investigation, operation of the adaptor, organisation of the operational exercises).

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 (through EMSA) 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?

Background

The EMFAF (2021-2027) provides funding to support the implementation of the Common Fisheries Policy (CFP) and the Union's maritime policy.

The general objectives of the EMFAF are to contribute to sustainable fisheries and conserve marine biological resources to ensure food security through the supply of fisheries and aquaculture products, the sustainable management of aquaculture, growth of a sustainable blue economy and healthy, safe, and sustainably managed seas and oceans.

The objectives fall under four priorities, which give a thematic and sectoral focus to the channeling of support under the EMFAF.

> **P1**: **Fostering sustainable fisheries and the restoration and conservation of aquatic biological resources (implementation of the CFP)**
>
> P2: Fostering sustainable aquaculture activities and marketing and processing of fishery and aquaculture products, thus contributing to food security in the Union (aquaculture, marketing and processing of fishery and aquaculture products)
>
> P3: Enabling a sustainable blue economy in coastal, island and inland areas and fostering the development of fishing and aquaculture communities (sustainable blue economy)
>
> **P4: Strengthening international ocean governance and enabling seas and oceans to be safe, secure, clean, and sustainably managed (international ocean governance)**

The use of EMFAF for CISE implementation

With a total available budget of €6.108 billion, the EMFAF fund is divided between the "shared management" and "direct management", offering stakeholders two different funding channels to co-finance the implementation of CISE:

- **Under shared management** through national EMFAF programmes by Member States based on national strategies (EUR 5.311 billion – 87%).

  Under the shared management, each Member State submitted their operational programmes which have been adopted by the Commission for the period 2021-2027, and can be found at the following webpage: EMFAF programmes 2021 - 2027 (europa.eu).

Carrying out many different operational surveillance tasks, national authorities directly benefit from being connected to CISE, in various sectors such as:

- safety and security of maritime transport
- fisheries control
- marine pollution preparedness and response
- protection of marine environment
- customs
- border control
- general law enforcement and
- defence

These benefits help reaching two of the specific objectives of the EMFAF:

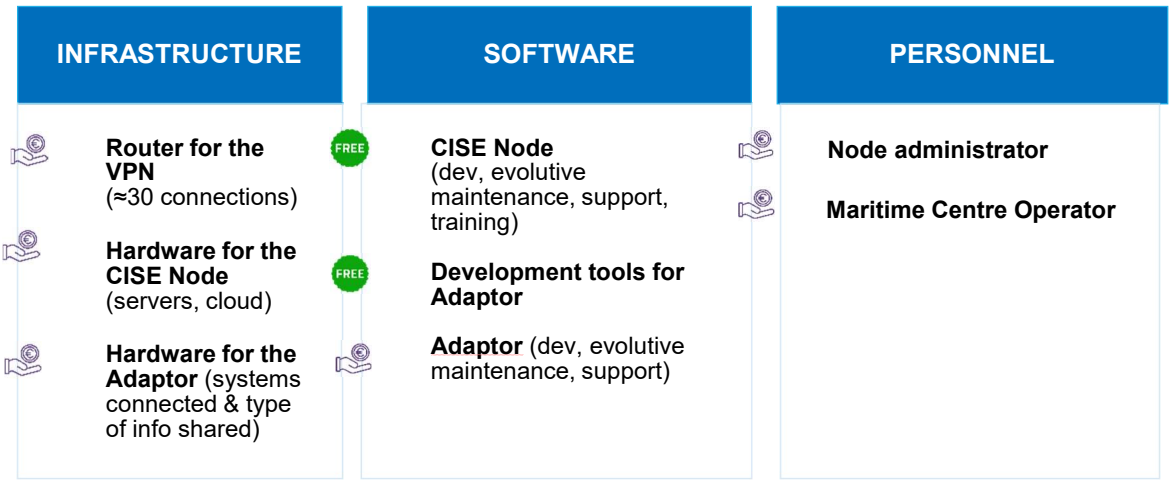
- **SO 1.4**: Fostering efficient fisheries control and enforcement, including fighting against Illegal, Unreported and Unregulated (IUU) fishing, as well as reliable data for knowledge based decision-making (data collection and control)

  SO 4.1: Strengthening sustainable sea and ocean management through the promotion of marine knowledge, maritime surveillance or coast guard cooperation (sustainable ocean management)

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.

Figure 7. CISE costs and the EMFAF financial support



	Possibly eligible for co-financing under EMFAF
FREE	Free of charge

Each Member State has designated a managing authority responsible for the EMFAF (national contact point). Therefore, each authority who would like a support for CISE under EMFAF should channel such request via the respective national EMFAF managing authority.

- **Under direct or indirect management** by the Commission (EUR 797 million – 13%).

  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 the pre-operational phase and to foster the uptake of CISE in view of its operationalisation.

  The grant was awarded to a project named "**CISE-ALERT**" coordinated by France (SGMer) and implemented by a consortium comprising authorities from Bulgaria (EAMA), Italy (ADM, ASI), Greece (HMOD), France (SHOM, DNGCD, MTE), Slovenia (SMA) and Portugal (DGPM, MDN), and, as partner authorities, from Finland (Finnish Border Guard) and the Netherlands (Ministry of Infrastructure and Water Management). The project aimed to launch CISE as an operational tool to increase the interoperability and enhance the cooperation of the EU actors involved in maritime surveillance operations by reinforcing the sharing of information among them. Further information related to the "CISE-ALERT" project can be found on the website of the project.

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

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 Technical and Operational Support

To support the activities in the CISE Network, EMSA provides a Technical and Operational support service to all the CISE stakeholders at no cost. Within this service, EMSA established an 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 at EMSA, which is organised in 3 levels:

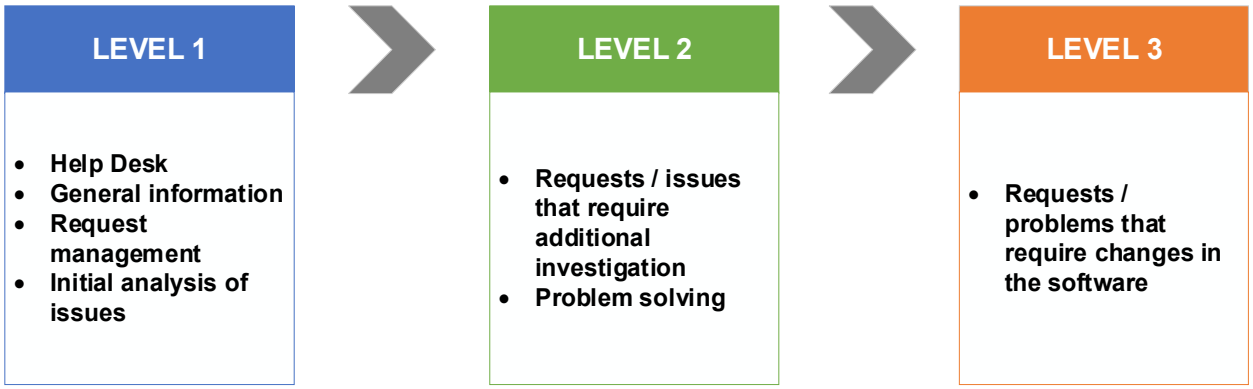


Figure 8. Support levels

CISE stakeholders may find more information about the Technical and Operational support service in the CISE Welcome Package.

5. Operational aspects

5.1 Information shared in the CISE network

When planning the connection to the CISE network, it is crucial to decide which information participants intend to provide and to consume from the network. It is important to highlight that CISE is a voluntary network which builds on the contribution from its participants. It is therefore of utmost importance that the MS authorities or EU Agencies interested in joining the network reflect not only on which information they want to receive through CISE, but also what information they have available and are willing to share that can be valuable to the other CISE participants that may have a legitimate use for it.

This is referred to as **Information Sharing Plan (ISP)** which captures the information that each participant intends to provide and consume in the CISE network via their own legacy system using the information services based on the CISE data and service model.

Knowing which kind of information is provided and consumed in the network, and by whom, is of foremost importance for each authority who intends to use CISE for their operations at sea. To this purpose, each CISE participant is invited to define and keep their own ISP updated, which is recorded in the so-called **CISE Catalogue**. This Catalogue is a living document which is distributed to the CISE stakeholders upon request as well as ahead of every CISE Stakeholders Group meeting so that all stakeholders are aware of which type of information can be consumed from the network.

5.2 Operational services

In the Transitional Phase of CISE (2019-2024), a dedicated working group composed by experts nominated by the CISE stakeholders - namely the "(Pre-)Operational Services Working Group" developed the first CISE operational services. Each of these services are defined by a specific workflow through which the information is exchanged among CISE participants using the CISE information services and data model in a specific operational context.

Without prejudicing any operational services provided under international, EU or national law, the following initial set of operational services were elaborated by the abovementioned working group to give the Member States the opportunity to supplement information available in their legacy systems:

Operational service	Operational use

Vessel of Interest (VOI) list	To gather information from the network regarding **vessels** considered **of interest** for safety, security or any other reason (e.g., vessel location, speed, flag, colour…).
Event Reporting (Incident)	To report an **incident** occurring on board of vessels, seaborne or airborne assets, or at any location in the EU maritime territorial waters (e.g., engine failure, collision…).
Risk Profile	To alert about **risks** in particular maritime geographical areas that may affect vessels, activities or the environment (e.g., illegal fishing, pollution…).
Request for Operational Assistance	To request **operational assistance** to other authorities operating in the area by benefitting from their asset support (e.g., maritime, aerial assets…) during a specific operation at sea.
Area of Interest (AOI)	To gather additional information in a specific defined **area** (e.g., satellite images, reporting on any illegal activities occurring in the area…).

5.3 Training and best practices

To enable the sharing of best practices and lessons learnt amongst the CISE Stakeholders, EMSA organises regularly training courses and themed workshops.

Moreover, an online training module has also been developed. The **Basic Online module** provides a general understanding about CISE, as well as information on how to join the CISE network. The online module is available on the CISE website and can be completed at one's own pace: https://www.emsa.europa.eu/cise/useful-material/interactive-guide.html

As to the training courses organised by EMSA, one that is recurrently offered is the Node Administrators Training. The topics addressed include 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 serves to connect node administrators from different stakeholders and to build a network through which best practices and problem-solving approaches can be tested.

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

6. Responsibility to share

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.

This proactive information sharing attitude is key to CISE as it will enable the further distribution of information within the CISE community. Ideally this should occur even when the information has not been specifically requested by another party. As a result of high value information reaching a higher number of authorities that have legitimate use for it, the overall performance of the national and 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 produce “pictures” of the information being shared in the moment and provide the framework to identify what could be useful to share in the future.

In this context, a methodology to support the Member States to implement the RTS principle was developed and tested. The methodology defines the criteria for measuring and promoting the sharing of information within the CISE network. To support this work, a dedicated RTS Working Group was set up in 2020, comprising experts nominated by the CISE stakeholders.

7. Communication

EMSA has established several communication channels for CISE stakeholders. The choice of channel or tool depends on the purpose of the information being shared, and they are designed to complement and support one another.

A dedicated section for CISE is set up on the EMSA’s website: www.emsa.europa.eu/cise.html. It serves as the main tool to share information about the latest news on CISE and upcoming events. The webpage helps also to disseminate communication and visibility material, such as a video on CISE, leaflet, infographics, etc.

The collaborative platform, set up in Microsoft Teams, is a 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 to 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