Practical Guide for joining the CISE network

Version 3.0

Funded by the European Union

Table of Contents

Introduction **4**

1. About CISE **4**
1.1 Political background 4
1.2 CISE key features 5
1.3 CISE Transitional and Operational Phases 5
1.4 Functionality of CISE 5
1.5 CISE network 6
1.6 Security 6
1.7 CISE Welcome Package 6

2. Organisational aspects **7**
2.1 Roles and responsibilities in the CISE network 7
2.2 Governance models 8
2.2.1 Model 1: “One CISE node – one adaptor” 9
2.2.2 Model 2: “One CISE node – more than one adaptor” 10
2.2.3 Model 3: “One country with more than one CISE node” 11
2.2.4 Model 4: “National node connected to the CISE node” 12

3. Financial aspects **12**
3.1 Costs 12
3.1.1 Infrastructure 13
3.1.2 Software 13
3.1.3 Personnel 13
3.1.4 Technical and Operational support for the adaptor 13
3.2 Funding opportunities 14
3.2.1 How can the EMFAF financially support the implementation of CISE? 14

4. Technical aspects **15**
4.1 Technical documentation 15
4.2 CISE Support Team 15
4.3 Standardisation 16

5. Operational aspects **16**
5.1 Information shared in the CISE network 16
5.2 (Pre-)Operational services 17
5.3 (Pre-)Operational exercises 17
5.4 Training and best practices 18

6. Responsibility to share **19**

7. Communication **19**

List of Figures

Figure 1. Main building blocks of the CISE decentralized architecture 6
Figure 2. Examples of governance models 8
Figure 3. Model 1. “One CISE node – one adaptor” 9
Figure 4. Model 2. “One CISE node – more than one adaptor” 10
Figure 5. Model 3. “One country with more than one CISE node” 11
Figure 6. Model 4. “National node connected to the CISE node” 12
Figure 7. CISE costs and the EMFAF financial support 15
Figure 8. Support levels 16
Figure 9. (Pre-)Operational Exercises 18

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
JRC	European Commission's Joint Research Centre
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**") 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 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 to those already actively involved in the network. The content of this guide will be subject to periodic updates to ensure its accuracy and relevance.

The guide is divided in 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.
- **Section 2**, **3**, **4** and **5** presents 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 procured study for an audit on the implementation of 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-sectors and cross-borders 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, 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 authority wants to connect to CISE (i.e., legacy systems) with its Adaptor. The Adaptor plays the crucial role to connect 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 December 2023 with the main aim to turn the EUCISE2020 project into a European-wide operational network open to all EU Member States and EU Agencies on a voluntary basis.

The main objective 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 pre-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) is setting up the **Operational Phase** of CISE with the aim of becoming fully implemented in the operational activities of maritime surveillance authorities. The Operational Phase starts in 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 information among authorities, CISE offers the following standard building blocks:

- The **CISE Node**, which is a common software for all the authorities connected to the network, allows the maritime authorities 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**, which 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.

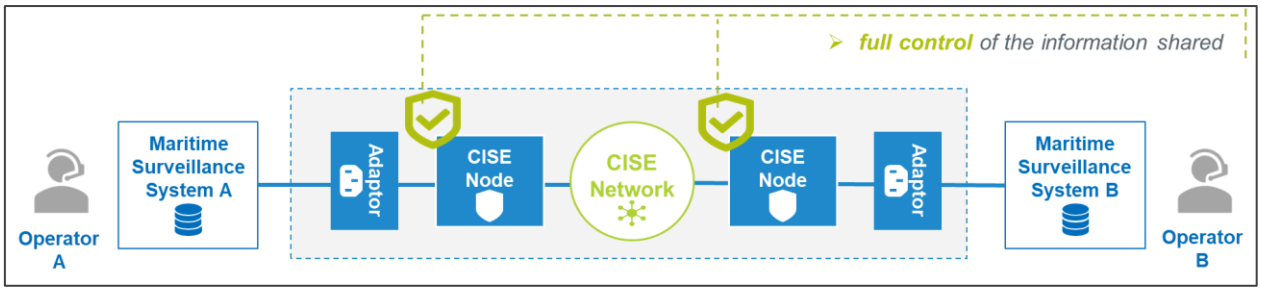


Figure 1. Main building blocks of the CISE decentralized architecture

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

1.5 CISE network

The composition of the CISE network changes over time adding new nodes, legacy systems and data. The most updated version of the CISE network diagram providing a snapshot of the network composition can be found at the EMSA's CISE website in the section CISE Network.

1.6 Security

The CISE security approach is based on the 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 recommendations 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 recommendations, 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 recommendations 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 are following the ISO 27001.

1.7 CISE Welcome Package

All relevant information about CISE such as the CISE Transitional Phase and - as of 2024 - of the Operational Phase activities and governance structure, the technical specifications of the CISE building blocks (CISE Node and adaptor), and how to request support or training from EMSA/JRC are included in the CISE Welcome Package which can 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 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 by 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 on 9 and 10 February 2021.

The Cooperation Agreement regulates the information sharing in the CISE network. By signing the Cooperation Agreement, authorities commit 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 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 as a "**Party"** to the Agreement. By signing, each Party will have to comply with all the stipulations and obligations contained in the Agreement.

In 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 providing, 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 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 its 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 sent 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 be also sent together with the copy of the Agreement.

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

- "**Node Administrator**" who will act as 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 (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.

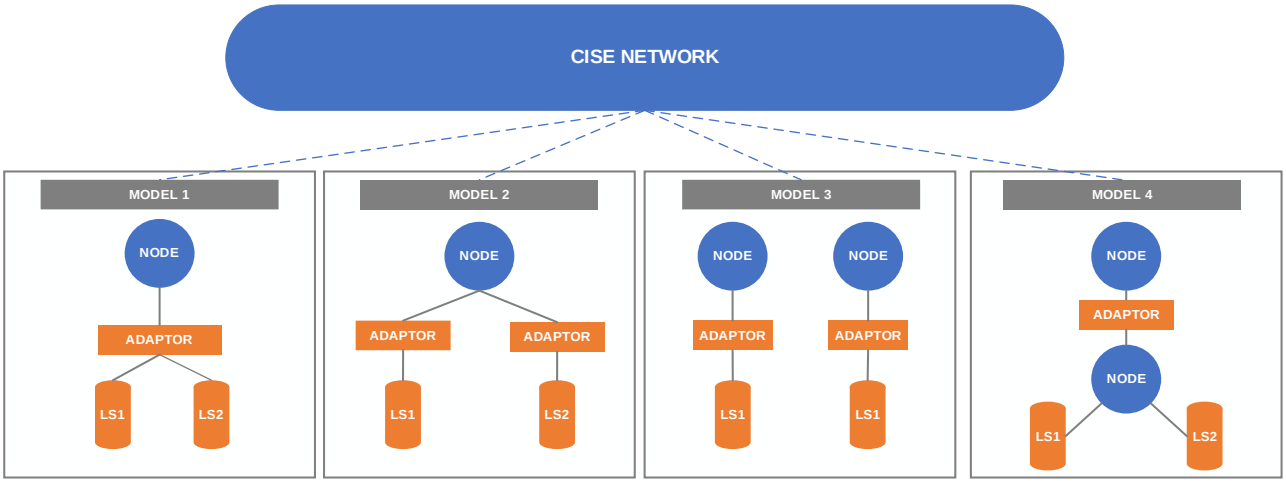


Figure 2. Examples of governance models

There is not one model that 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”

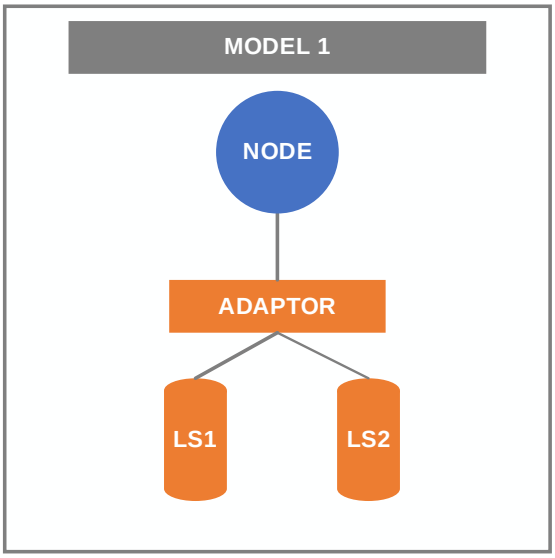


Figure 3. Model 1. “One CISE node – one adaptor”

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

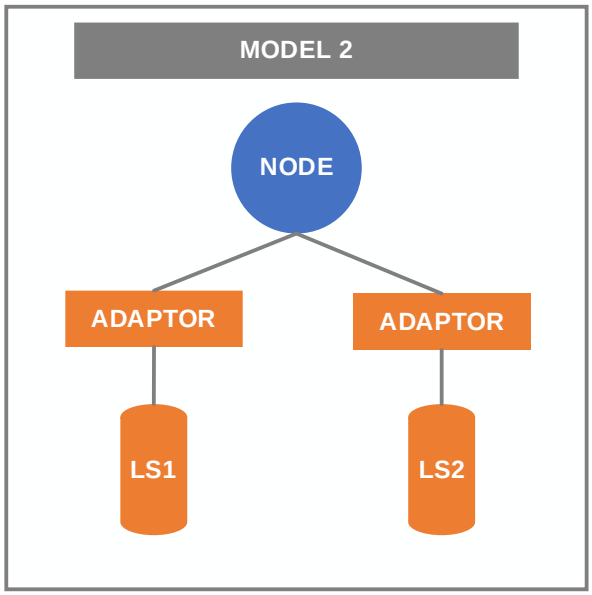


Figure 4. Model 2. “One CISE node – more than one adaptor”

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

Pros	The adaptor responsibility is easier to target when it relates to one legacy system only.
Cons	Each authority that wants to connect their legacy systems has to procure its own adaptor.
This model is recommended where the number of the authorities that need to connect their legacy systems is 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”

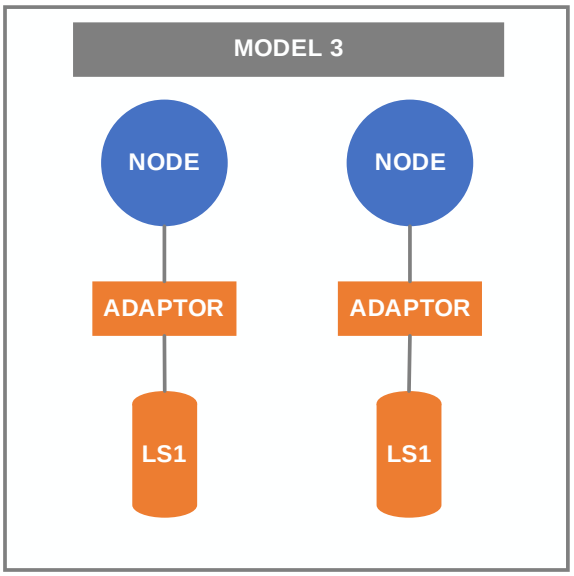


Figure 5. Model 3. “One country with more than one CISE node”

Governance Model 3 can be suitable for a country having two separate nodes, governed by two different public authorities 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 of the adaptor is easier to be defined when it relates to one legacy system only.
Cons	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 CISE or in the information to share.	

2.2.4 Model 4: “National node connected to the CISE node”

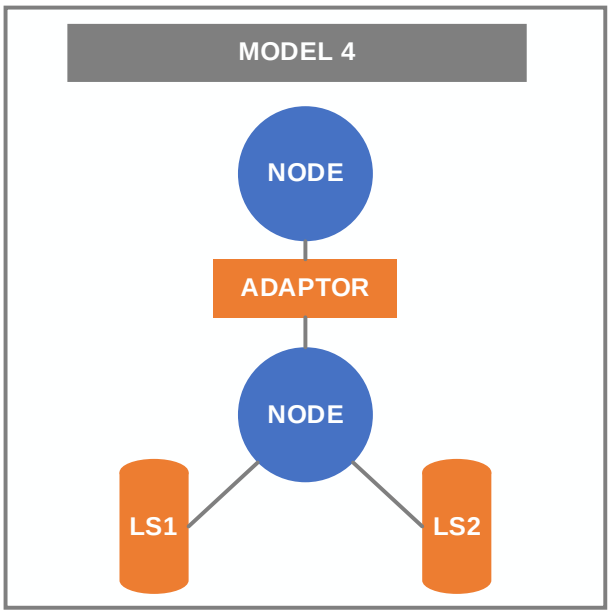


Figure 6. Model 4. “National node connected to the CISE node”

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 as shown in the figure above.

Pros	▪ 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.
Cons	▪ 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 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 CISE services to be developed;
- 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:

1. The **infrastructure**;
2. The **software**;
3. 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 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 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**. Node software is free of charge. 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.

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 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, 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 (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 EMFAF fund is divided between the "shared management" and "direct management", offering stakeholders two different funding channels to co-finance the implementation of CISE.

- Shared management

  Under the "shared management", €5.311 billion is provided to the Member States[1] which are invited to draft and submit to the Commission for approval their national programme, namely their public investment plan covering the EMFAF programming period (2021-2027) and their 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*"[2], 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.

  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 the implementation of CISE.

  The 2021-2027 EMFAF national programmes which were submitted by MS can be found at the following webpage: EMFAF programmes 2021 - 2027 (europa.eu).

- 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).

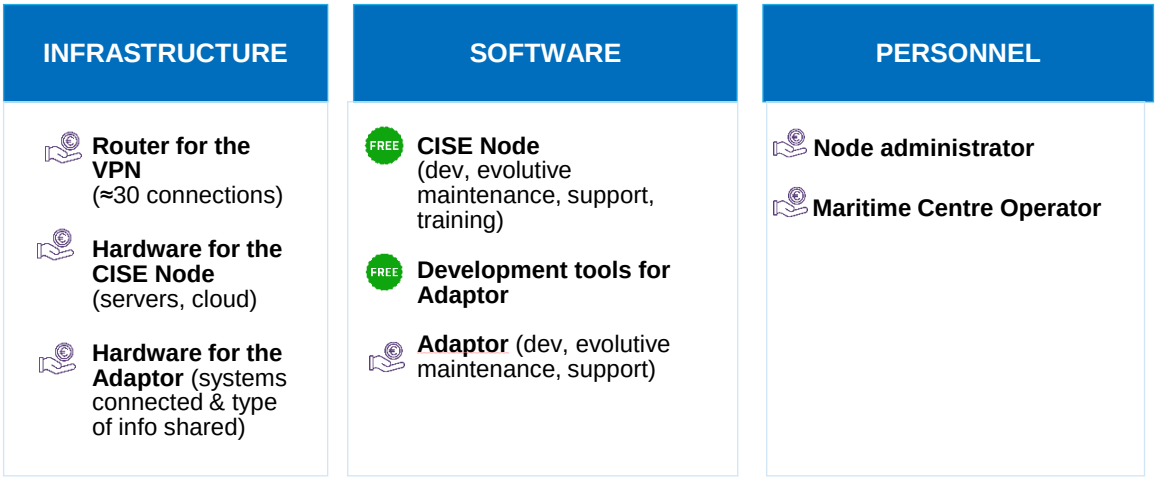
  In the context of CISE, the first call for proposal "Action for a CISE incident alerting system" was launched on 26 August 2021 by the European Climate, Infrastructure and Environment Executive Agency (CINEA) with the aim to co-finance one single project to enhance the cooperation between public maritime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

[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').
[2] The text of the Regulation 2021/1139 of the EMFAF can be found at this link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1139.

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). With a duration of 24 months starting from 1 November 2022, the project aims 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 Linkedin page of the project.

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

Figure 7. CISE costs and the 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, 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:

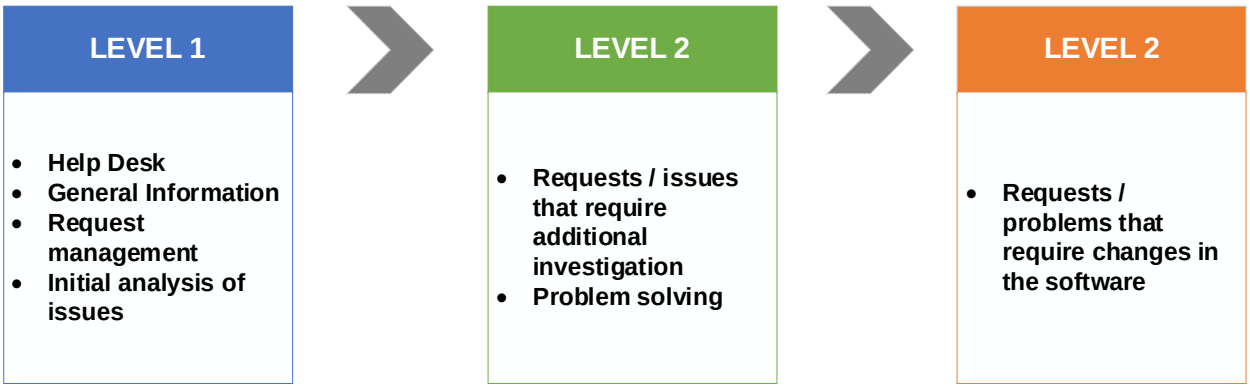


Figure 8. Support levels

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 in the CISE network

When planning the connection to the CISE network, it is crucial to decide which information participants intend to provide to and 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 which can be valuable to the other CISE participants that may have a legitimate use of 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 its own ISP updated, which is recorded in the so-called **CISE service 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 (Pre-)Operational services

One of the main objectives of the CISE Transitional Phase is to develop data exchange services to be tested and rolled-out in the pre-operational network and upon which the operational phase of CISE will be built.

To this purpose, a dedicated working group composed by experts nominated by the CISE stakeholders - namely the "(Pre-)Operational Services Working Group" - was established with the aim to develop and promote the implementation of such services. Each of these services is defined by a specific workflow through which the information is exchanged among CISE participants using the CISE services and data model.

During the Transitional Phase (2019-2023), the following initial set of operational services were elaborated by the abovementioned working group:

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 (Pre-)Operational exercises

With the purpose to test and roll-out the operational services elaborated by the dedicated Working Group (see section 5.2) in the CISE pre-operational network, a series of (pre-)operational exercises were initiated with different stakeholders as presented in the table below:

EXERCISE	OBJECTIVE
CISE TRIALS	To test the feasibility, correctness and exhaustiveness of the operational services elaborated and to train duty officers and node administrators to use CISE in their maritime operations centres (MOCs).
SEA BASIN EXERCISES	To prioritize the implementation of the operational services among countries from the same EU sea basins facing common maritime threats (i.e., threats to the critical infrastructures, hybrid threats, drug trafficking, unexploded ordenance, accidents at sea, etc.).

ANTI-DRUG TRAFFICKING	To conduct an information exchange exercise based on the anti-drug trafficking scenario agreed among involved law enforcement authorities.
CISE-ALERT	Testing and rolling-out the operational services in the framework of the CISE-Alert project

Figure 9. (Pre-)Operational Exercises

5.4 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, an online training module has also been developed.

During the CISE Transitional Phase (2019-2023), 12 workshops (see Figure 9) and 10 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
	EMD 2021 – CISE Workshop	21 May 2021
	EMFAF Workshop	30 September 2021
	MARSUR Workshop	13 October 2021
	Workshop with Customs	04 May 2022
	EMD 2022 – CISE Workshop	19 May 2022
	CISE-Industry Webinar	29 September 2022
	Adriatic Sea Workshop	11 May 2023
	EMD 2023 – CISE Workshop	24 May 2023
	CISE workshop for anti-drug trafficking operations	30 & 31 May 2023

Figure 9. CISE Workshops

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 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
	4th Node Admin Training	11 & 12 May 2022
	1st Virtual Open Day	21 September 2022
	Online Module (Basic)	October 2022
	5th Node Admin Training	23 & 24 November 2022
	2nd CISE Open Day	20 September 2023
	MOC Staff Information Session	25 & 26 October 2023

Figure 10. CISE Training courses

As to the online training module, the **Basic Online module** is available on the CISE website and can be completed at one's own pace. The online module provides a general understanding about CISE, as well as information on how to join the CISE network.

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 the 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.

This 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. As a result of high value information reaching the authorities that have legitimate use for it, 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 produce “pictures” of which information is being shared in the moment and provide the framework to identify what could be useful to share in the future.

In this context, a study has been procured to define a methodology to support the Member States to implement the RTS principle by identifying weaknesses and gaps, as well as 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 Member States nominating members, to support and advise on the design of this study. By 2021 the study was procured and at the beginning of 2022 the first draft Audit Methodology was provided by the contractor. To test the prescribed tools, and to further refine the methodology, two sets of revision exercises were carried and completed by 2023.

7. Communication

EMSA has arranged a number of communication channels for the CISE stakeholders. 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 the EMSA’s website: www.emsa.europa.eu/cise.html. It serves as the main tool to share information on the latest news on CISE and upcoming events. The webpage serves 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 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