EUROPEAN
COMMISSION

Strasbourg, 15.12.2015
C(2015) 9206 final

ANNEX 1

ANNEX

to the

COMMISSION RECOMMENDATION

adopting the Practical Handbook for implementing and managing the European Border Surveillance System (EUROSUR Handbook)

Table of content

1 Introduction

This handbook provides general, technical and operational guidelines as well as recommendations and best practice for implementing and managing the European Border Surveillance System (EUROSUR) established by Regulation (EU) No 1052/2013.[1]

This handbook is for the Member States, the European Agency for Management of Operational Cooperation at the External Borders of the Member States of the European Union ('the Agency') and the other EU bodies, offices and agencies involved in EUROSUR.

This handbook does not create any legally binding obligations upon Member States, the Agency or other EU bodies, offices or agencies, nor does it establish new rights and duties for national authorities who are responsible for border surveillance or any other bodies to whom the handbook might be relevant. Only Regulation (EU) No 1052/2013, on which this handbook is based, or other legislation it refers to,[2] can produce legally binding effects and can be invoked before a national court or tribunal.

This handbook is reviewed on a regular basis, in light of experience and lessons learned through implementing Regulation (EU) No 1052/2013.

[1] Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR).

[2] E.g. Regulation (EC) No 562/2006 of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), Charter of Fundamental Rights of the European Union.

2 General guidelines

2.1 Objectives and framework of EUROSUR[3]

EUROSUR is a multi-purpose system used for detecting, preventing and combating illegal immigration and cross-border crime at the external borders, thereby contributing to the further development of the Schengen *acquis*. It aims to contribute to protect and save the lives of migrants attempting to cross the external borders.

To achieve these objectives, EUROSUR provides a common *framework* for information exchange and cooperation among all authorities with responsibility for the surveillance of the external land and sea borders.[4] EUROSUR follows an intelligence and risk analysis driven approach, allowing national and European authorities to better understand what is happening at the external borders and enabling them to react faster to new routes and methods used for illegal immigration and cross-border crime. Key elements of this include near-real time information exchange, regular intelligence sharing and close cooperation among authorities at national and European level.

The *EUROSUR framework* consists of several components[5] which interrelate as follows:

At national level, authorities cooperate via *national coordination centres* for border surveillance and exchange information via *national situational pictures*. At European level, the national coordination centres exchange information with each other and the Agency via the *EUROSUR communication network*, with unlimited access to the *European situational picture* and the *common pre-frontier intelligence picture*.

The Agency also cooperates with other EU bodies, offices and agencies (e.g. European External Action Service, Europol, Eurojust, Fundamental Rights Agency) in order to make best use of the information, capabilities and systems available. For example, the Agency coordinates the *common application of surveillance tools* in cooperation with the European Maritime Safety Agency and the EU Satellite Centre to supply the national coordination centres and itself with surveillance information on the external borders and on the pre-frontier area.

EUROSUR allows Member States to react faster to incidents and to critical situations occurring at the external borders. To help with this, the external land and sea borders are divided into 'border sections', each of which is given an impact level. This approach allows hotspots at the external borders to be identified, with a standardised reaction at national level and support from the Agency if required.

To achieve EUROSUR's objectives, Member States also exchange information and work with neighbouring third countries based on agreements and through specific regional networks based on those agreements.

When exchanging information and cooperating in the framework of EUROSUR, Member States and the Agency must comply with requirements to protect fundamental rights, in particular the non-refoulement principle and the protection of personal data.

[3] Articles 1 and 4 of Regulation (EU) No 1052/2013.

[4] The EUROSUR framework may also be used for the surveillance of air borders and for border checks if Member States voluntarily provide such information to EUROSUR.

[5] National coordination centres, national situational pictures, EUROSUR communication system, European situational picture, Common pre-frontier intelligence picture, common application of surveillance tools – see Article 4 of Regulation (EU) No 1052/2013.

2.2 Scope[6]

Topic	In scope	Optional	Out of scope
Border control (surveillance and checks)	• Surveillance of external land and sea borders[7]	• Surveillance of external air borders • Checks at border crossing points	• Internal borders
Border surveillance	• Monitoring • Detection • Identification • Tracking • Prevention • Interception	-	Legal and administrative measures after interception (e.g. asylum procedures, readmission, return, judicial investigations)
Situational awareness[8]	• Events, information and analysis on:[9] – Unauthorised border crossings – Cross-border crime – Risk to migrants' lives • Position, status and type of – assets of national authorities with a responsibility for external border surveillance in the national situational picture (NSP) – assets of the Agency in the European situational picture (ESP) and common pre-frontier intelligence picture (CPIP)	Position, status and type of assets on a border surveillance/ law enforcement mission operating in the neighbouring external border sections of another Member State	Position, status and type of military assets which are not assisting a law enforcement mission
Reaction capability	• Unauthorised border crossings • Cross-border crime	-	Coordination of search and rescue operations at sea
Personal data	Personal data relating to ship identification numbers in the ESP/CPIP	Personal data in the NSP	Any other personal data in the ESP/CPIP

[6] Article 2 of Regulation (EU) No 1052/2013.
[7] Including temporary external borders.
[8] With regard to the external sea borders, EUROSUR is supporting the development of the common information sharing environment (CISE) for monitoring the EU's maritime area. Once established, CISE will provide a wider framework for maritime situational awareness by supporting information exchange among public authorities across sectors, ranging from maritime safety and security to fisheries control, marine environment protection, customs, border control, general law enforcement and defence.
[9] The provisions in this handbook do not alter any requirements for national authorities to share information through other dedicated systems based on EU legislation (e.g. customs authorities, via the community customs risk management system, based on Commission Regulation (EEC) No 2454/93).

2.3 Definitions for the purposes of this handbook[10]

1) 'Monitoring' means observing a situation or geographical area.
2) 'Detection' means becoming aware of an object of interest's presence and location.
3) 'Identification' means establishing the unique identity or specific characteristics of the object of interest.
4) 'Tracking' means determining the past, current and future locations of an object of interest.
5) 'Prevention' means activities that hinder or prevent an action from taking place.
6) 'Interception measures' means measures taken to prevent the object of interest from proceeding further.
7) 'National authorities' means all authorities with responsibility for surveillance of the external land and sea borders in accordance with national law and, if applicable, with responsibility for border checks and air border surveillance.
8) 'National border surveillance system' means a single structure or a combination of surveillance and monitoring systems which brings together surveillance activities at the external borders of a Member State, under the coordination of the national coordination centre in accordance with national law, and supports the exchange of information between all national authorities with responsibility for external border surveillance.
9) 'Own assets' means the mobile or stationary equipment and human resources at the disposal of a Member State or the Agency used to monitor and patrol the external borders.
10) 'Status of assets' means the level of readiness and the availability of the asset.
11) 'Event' means either an incident (a situation relating to illegal immigration, a cross-border crime or a risk to the lives of migrants) or a crisis situation (for instance in a neighbouring third country) or any other situation which has a significant impact on border security.
12) 'Unauthorised border crossings' refers to any act of crossing the border at or outside border crossing points which is not in compliance with the rules for crossing the external borders set out in the Schengen Borders Code.
13) 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
14) 'Processing of personal data' means any handling which is performed upon personal data, whether by automatic means or not, including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmitting, disseminating or otherwise making the data available, alignment or combination, blocking, erasure or destruction.
15) 'Neighbouring third country' means a third country which has either a land or sea border or a common sea basin with a Member State.

[10] See Article 3 of Regulation (EU) No 1052/2013. Definitions relating to the processing of information are to be used as defined in the Common Integrated Risk Analysis Model (CIRAM) v.2.0.

2.4 Protection of fundamental rights and measures contributing to saving migrants' lives[11]

1. National authorities comply with international and European instruments on fundamental rights,[12] and in particular the EU asylum acquis and international refugee law. They respect the human dignity of persons involved in illegal immigration and cross-border crime and must not discriminate on the grounds of sex, race, social condition or ethnic origin, language, religion or belief, political or any other opinion, disability, age or sexual orientation. Any measures taken while carrying out their duties must be proportionate to the objectives pursued by such measures.
2. When collecting information during border surveillance activities, the right to private life and the protection of personal data of any persons must be respected, in accordance with national and EU legislation.
3. The authorities observe their obligation to render assistance to any vessel or person in distress at sea and, during a sea surveillance operation, ensure that their participating units comply with that obligation, in accordance with international law and respecting fundamental rights. In the context of operational cooperation coordinated by the Agency, they adhere to the rules established by Regulation (EU) No 656/2014[13]
4. Whenever persons are in need of medical assistance, including pregnant women or injured, sick or dehydrated people, the coordination centre responsible (Maritime Rescue Coordination Centre, local, regional or national coordination centre, depending on the situation) must ensure that the necessary measures, such as requesting medical support, are taken without delay. The safety of the crew and the people in question is of paramount concern and all measures must be conducted in a way that ensures such safety, at all times.
5. Border guards and staff from all relevant national authorities are trained in how to identify and approach children and vulnerable people[14] and assist those people in accessing the appropriate protection or assistance measures.[15] Staff is provided with information on national referral mechanisms[16] and on how to preserve evidence of crimes at the border for possible future legal proceedings.
6. National authorities ensure, in full compliance with the principle of *non-refoulement*, that people seeking international protection are identified, receive adequate assistance, are informed appropriately about their rights and how to access relevant procedures (including the possibility of requesting asylum), and are promptly referred to the national authorities responsible for receiving their asylum requests.

[11] Article 2(4) of Regulation (EU) No 1052/2013.
[12] This includes the Convention for the Protection of Human Rights and Fundamental Freedoms; the Charter of Fundamental Rights of the European Union; and the 1951 Convention Relating to the Status of Refugees and its 1967 Protocol.
[13] Regulation (EU) No 656/2014 of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union.
[14] E.g. pregnant women, women with small children, unaccompanied minors, people susceptible to exploitation and victims of exploitation or trafficking in human beings. See also VEGA Children Handbook (Frontex, 2015) and *Guidelines on the identification of victims of trafficking in human beings in particular for consular services and border guards* (European Commission, 2013),
[15] See Chapter 1.7 of the Common Core Curriculum.
[16] E.g. for victims of trafficking in human beings and for the protection of children.

7. In order to contribute to ensuring the protection and saving the lives of migrants at sea, there need to be in place national communication channels and workflows between the National Coordination Centre (NCC) and the Maritime Rescue Coordination Centre (MRCC) to ensure the timely exchange of information. This information exchange should take place taking full account of the fact that the MRCC is exclusively responsible for coordinating any operation relating to a search and rescue (SAR) incident, acting under specific SAR international legal instruments.[17] This information exchange could include:

   a) Information about the status and position of patrolling assets (important to both centres for assessing their reaction capability).

   b) Risk analysis products shared by the NCC with the MRCC, since migratory flows can lead to potentially high risks for lives at sea.

   c) The MRCC and NCC may share with each other their satellite and terrestrial communication and tracking capacities, incl. ones which are available via the Agency.

   d) Informing the MRCC about incidents that do not initially require, but might later on need, SAR actions so that they are ready to respond in case conditions worsen and SAR action is required. Similarly, the NCC should be informed about any SAR incidents involving migrants.

   e) The NCC may assist the MRCC in selecting the disembarkation point, if one is needed (the decision on this during SAR operations must be made by the MRCC). This may be of relevance to allow further arrangements (such as local administrative and hosting reception capacity at disembarkation) to be made.

Best practice: The MRCC and NCC conclude a formal agreement on information exchange in accordance with data protection rules, thereby ensuring smooth cooperation. This may cover, for example, the deployment of liaison officers, the list of products and reports to be exchanged, possible access to each other's IT systems (on a need-to-know basis and in line with national data protection rules) and regular meetings between the staff from the two centres at both management and working level.

Patrol assets used for border surveillance operations should be equipped for SAR operations.

8. When cooperating with a neighbouring third country, Member States comply with their obligations under EU and international law, in particular with the principle of non-refoulement and data protection rules. They must not share any information which could be used by the third country to identify persons or groups of persons whose request for access to international protection is under examination or who are at serious risk of being subjected to torture, inhuman and degrading treatment or punishment, or any other violation of fundamental rights.

Best practice: The NCC draws up a standard operating procedure for sharing information with third countries. This procedure should include checking that information is not shared when the NCC knows or is supposed to know that it will be or most likely might be used by the third country to violate fundamental rights. An electronic log could be kept with the date, the name of the third country and the type of information shared.

[17] 1979 International Convention on Maritime Search and Rescue and other International Conventions falling under the auspices of the International Maritime Organisation.

3 Operational guidelines

3.1 National Coordination Centre[18]

3.1.1 Functions and tasks

The NCC coordinates and exchanges information among all national authorities with responsibility for the surveillance of the external land and sea border, as well as with the other NCCs and the Agency. The NCC's organisational structure and staffing varies to suit national circumstances, in particular the impact levels attributed to external border sections and how the NCC is integrated in the authority that hosts it. The NCC's activities are managed by the Head of the NCC. Its functions and tasks are as shown in the table below.

Functions	Tasks[19]
Management	– Monitor and supervise NCC activities, incl. compliance with fundamental rights – Manage and administer NCC staff – Ensure NCC security (personnel, building, ICT)
Situational awareness and risk analysis	– Create and disseminate the NSP; in this context – Monitor the operational situation at the external border and collect operational and strategic information – Collect, process, evaluate, validate, filter and fuse situational information (incidents, assets, intelligence[20]) at national level – Translate and create artefacts in the NSP application – Analyse patterns and trends in illegal immigration and cross-border crime – Develop and manage intelligence requirements and produce risk analysis products shared in the NSP, ESP and CPIP to support decision-making
Reaction capability[21]	– Monitor the efficient implementation of operational activities at local/regional level and evaluate national performance; in this context – Ensure authorities at local/regional level work smoothly together – Assess the need for additional assistance at local/regional level – Evaluate national operations and contributions to joint/bilateral operations
Liaison	– Agree working and liaison arrangements with national authorities – Contact with liaison officers' network – Support from/to the Agency (National Frontex Point of Contact/NFPOC)
Planning	– Support national border management planning and capacity building – Support the planning of long-term surveillance activities
ICT	– Operate, monitor, support, maintain and further develop ICT systems
Availability	– NCC staff ensure the 24/7 operational availability (e.g. during night shift) – Contact management in case of emergency – Create and maintain phone lists and checklists

[18] Article 5 of Regulation (EU) No 1052/2013.

[19] These tasks can either be carried out by the NCC itself or by other national authorities or bodies in the national authority hosting the NCC, as long as they work with the NCC.

[20] This may include Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Imagery Intelligence (IMINT) and Signals Intelligence SIGINT).

[21] The relevant national authority is responsible for the command and control of assets and resources. The NCC has a coordinating and strategic role and, depending on the way responsibilities have been divided at national level, may have also an operational role.

NCC staff needs to have sufficient foreign language skills to be able to work with neighbouring and other NCCs. The NCC needs to have enough qualified internal or external translation capacity to ensure the timely exchange of information.

When a Member State hosts an operational activity coordinated by the Agency (e.g. a joint operation), it may use the infrastructure provided by the NCC or subordinated centres.

3.1.2 National authorities responsible for border surveillance[22]

In order to coordinate their activities, representatives from the national authorities with responsibility for the surveillance of the external land and sea borders work together in the NCC on a permanent basis.

The NCC may also provide information on the surveillance of air borders and on checks at border crossing points if Member States decide it. In this case, it is recommended that representatives from the national authorities responsible for border checks and air border surveillance also work in the NCC.

The NCC may include liaison officers from other national authorities or other relevant bodies, as needed.

3.1.3 Cooperation with other national authorities[23]

Depending on the national division of responsibilities and without prejudice to any obligations under the legislation governing their activities, the NCC exchanges information and cooperates on a regular basis, through the appropriate channels, with the following national authorities:

a) Coastguard
b) Police/gendarmerie
c) Customs authorities[24]
d) National guard
e) Armed forces
f) Maritime rescue coordination centre (MRCC)
g) Migration authorities
h) Asylum authorities

The NCC may exchange information and cooperate, through the appropriate channels, with other national authorities, including:

a) Maritime authority
b) Fishery control authority
c) Liaison officers posted abroad
d) Veterinary/phyto-sanitary services

[22] Article 5(3)(a) and Article 2(2) of Regulation (EU) No 1052/2013.
[23] Article 5(3)(b) of Regulation (EU) No 1052/2013.
[24] See Article 4(3) of Council Regulation (EEC) No 2913/92 and Articles 3 and 5(1) of Council Regulation No. 952/2013 (Union Customs Code, applicable on 1.5.2016). Given their role in the supervision of the movement of goods moving across the external borders and their responsibilities for risk analysis and risk management, customs authorities may nominate representatives to work in the NCC.

e) Prosecutor's office

f) Consular department of the Ministry for Foreign Affairs, embassies and consulates

g) SIRENE Office

h) Authorities responsible for preventing nuclear proliferation

i) Transport authorities

j) Civil protection services

k) Environmental protection services

l) Intelligence services

m) Authorities responsible for referral mechanisms for victims of trafficking in human beings and for protection systems for other vulnerable groups, such as children.

n) Health authorities

3.1.4 Management of resources and personnel[25]

The NCC supports the effective management of resources and personnel by national authorities with responsibility for external border surveillance. In so doing, the NCC supports the planning and implementation of border surveillance activities, including by:

a) Establishing and updating an *overview of all available assets* belonging to national authorities responsible for border surveillance, including the assets' level of readiness, type and use in the operational layer of the NSP.

b) Coordinating that assets available at national level are distributed to the border sections corresponding to the impact levels allocated to those sections.

   This may include *reallocating assets* provided by one national authority from one border section to another one, or *allocating additional assets* provided by another national authority to reinforce the surveillance measures taken at a given border section.

   To do this, the NCC ensures that the necessary workflows and arrangements are in place to allow for assets to be reallocated quickly, with the agreement of the relevant national authorities.

c) Contribute to national *capacity building for border surveillance and, if applicable, border checks*, by working closely with the relevant national authorities. This may include identifying gaps and needs relating to:

   – information collected from different systems, sensors, patrols and other sources;

   – skills and tools for analysing information;

   – stationary and mobile assets;

   – appropriate personnel availability and profiles;

   – training, including training for NCC staff.

d) Support the *planning, implementation and adaptation of operations* at local, regional and national level as well as at EU level in cooperation with the Agency. This may include issues such as communication, procurement of interoperable equipment and a national border control strategy.

[25] Article 5(3)(c) of Regulation (EU) No 1052/2013.

3.1.5 National situational picture[26]

The NCC creates and maintains the NSP by processing and evaluating situational information, managing the national intelligence process and developing analytical products in line with the provisions of Chapter 3.2 of this handbook. The NCC shares information regularly with the relevant national authorities via the NSP.

3.1.6 Planning and implementation of national surveillance activities[27]

The NCC supports the planning and implementation of national surveillance activities by monitoring surveillance activities at local, regional, national and EU levels, and provides suggestions on adjusting practices based on experience.

3.1.7 National border surveillance system[28]

Each Member State with external land and sea borders creates and maintains a national border surveillance system, consisting of a single structure or a combination of national surveillance and monitoring systems. Surveillance activities at each external border section correspond to the impact level allocated to it (see Chapter 3.3.6.), using stationary and mobile equipment and patrols.

The NCC coordinates the national border surveillance system in accordance with national law by monitoring the system's functioning, including the impact levels allocated and the operational procedures, and provides input into developing the system and procedures.

The NCC has direct and real-time access to the relevant parts of the national border surveillance system, including sub-systems set up at local/regional level and surveillance systems managed by other national authorities. If the NCC receives information on a border section from two or more national surveillance systems, it combines this information.

3.1.8 Effect measurement[29]

The NCC supports the regular measuring of the effects of national border surveillance activities, by collecting and analysing information and producing an overview of events and response activities carried out, including their effectiveness and the resources and personnel used.

3.1.9 Cooperation with other NCCs[30]

Within EUROSUR, the NCC is the single point of contact for exchanging information and cooperating with other NCCs and with the Agency.

3.1.10 Operating hours[31]

The NCC operates twenty-four hours a day and seven days a week, ensuring the presence of at least a duty officer/shift commander.

[26] Article 5(3)(d) of Regulation (EU) No 1052/2013.
[27] Article 5(3)(e) of Regulation (EU) No 1052/2013.
[28] Article 5(3)(f) of Regulation (EU) No 1052/2013.
[29] Article 5(3)(g) of Regulation (EU) No 1052/2013.
[30] Article 5(3)(h) of Regulation (EU) No 1052/2013.
[31] Article 5(4) of Regulation (EU) No 1052/2013.

3.1.11 Notification of NCC establishment and monitoring[32]

Each Member State must notify the European Commission that its NCC has been established. The Commission regularly provides Member States and the Agency with a technical report on the establishment and development of the NCCs.

The NCC regularly informs the Agency of relevant developments regarding its activities and structures. This may include information on additional responsibilities, functions and tasks given to the NCC, additional authorities who cooperate with the NCC, technical upgrades or any other relevant information.

3.1.12 Allocation of tasks to other national authorities[33]

Member States may charge regional, local, functional or other authorities with ensuring situational awareness and reaction capability in their respective areas of competence on condition that:

1) they are in a position to take operational decisions;
2) the tasks allocated support the effective and efficient management of resources and personnel, support the planning and implementation of national border surveillance activities or help coordinate the national border surveillance system; and
3) this decision does not affect the NCC's ability to cooperate and exchange information with other NCCs and the Agency.

In pre-defined cases, the NCC may authorise regional, local, functional or other authorities to communicate and exchange information with regional authorities or the NCC in another Member State or the responsible authorities in a third country, as long as they regularly inform the NCC about their communication and information exchange.

When coordinating border surveillance activities with functional and other authorities, the NCC ensures that the responsibilities and autonomy (e.g. command and control functions) of each of these authorities are fully respected.

3.1.13 Internal rules of procedure

The authority responsible for the NCC has internal *rules of procedure*, detailing the process to follow for exchanging information and working with relevant national authorities. These rules also cover the handling, storing, transmission, processing and deleting of personal data and non-classified sensitive and classified information.

3.1.14 Interagency cooperation at national level

Each Member State determines the split in responsibilities among its national authorities that are responsible for external border surveillance. National authorities must respect each other's areas of responsibility and refrain from taking any actions which might directly or indirectly impact on other authorities fulfilling their tasks.

While there is no single model for interagency cooperation, improved cooperation, in particular between civilian and military authorities, allows for more effective and cost-efficient use of information, capabilities and systems available at national level.

Depending on the scope of the cooperation and the responsibilities of the relevant authorities as set out in national law, this cooperation may consist of:

[32] Article 5(1) and Article 22 of Regulation (EU) No 1052/2013.
[33] Article 17 of Regulation (EU) No 1052/2013.

a) *Information sharing:* National authorities share information derived from their individual systems as well as from the events, operational and analysis layer of the NSP. National authorities may also share information derived from their surveillance infrastructure (e.g. radar stations, monitoring of VHF frequencies) at local level, preferably in near-real time.

b) *Cooperation:* National authorities may share selected surveillance infrastructure (including establishment and maintenance e.g. of radar stations), provide controlled access to each other's systems and databases (on a need-to-know basis), carry out joint risk analysis, and coordinate their patrolling activities. National authorities should use the NCC as far as possible for this.

c) *Assistance:* One national authority (e.g. military authority) may provide assistance to another (e.g. border guard) in carrying out border surveillance tasks. Responsibility and authority to carry out the task remain with the original body. The relevant national authorities must inform the NCC about the scope, duration and other relevant information of the assistance measure.

d) *Integration:* In the best case scenario, a single national system and/or a single national centre are used by different national authorities to carry out different surveillance functions (e.g. border control, fishery control, search and rescue). Another possibility is that national law makes one national authority responsible for carrying out several surveillance tasks.

Various forms of cooperation can be envisaged:

→ *Personnel* from one national authority provide operational, analytical, technical and administrative information and support to another national authority;

→ Surveillance and communication *infrastructure* is shared to improve overall situational awareness;

→ Use of *equipment* (e.g. assets for patrolling) is coordinated to improve overall reaction capability;

→ *Standard operating procedures* for information exchange and cooperation are in place;

→ *Training* is provided to personnel in other authorities, leading to better mutual understanding and knowledge transfer.

Agreements between the relevant national authorities should clarify the scope of and arrangements for the cooperation as well as the legal, operational and financial obligations of each partner. Preference should be given to using or adapting existing agreements before concluding new agreements.

3.1.15 Contact list

The NCC creates and maintains a contact list of the national authorities with which it works and exchanges information.

3.2 Situational awareness

3.2.1 Relationship between situational pictures and their layers[34]

The national situational picture (NSP) maintained by the NCC provides situational awareness at national level, while the European situational picture (ESP) and common pre-frontier intelligence picture (CPIP) maintained by the Agency provides situational awareness at the European level. The relationship between these pictures and their place in the EUROSUR framework can be described as follows:

1) NSP

NCCs are responsible for creating and maintaining the NSP in each Member State. This is the sum of all information provided by that Member State to EUROSUR and thus reflects the origin of data, information and intelligence contained in them. The NSP can be created using technical platforms that are able to handle the information exchange required, enabling the Member State to supply relevant information in near-real time to the European situational picture and common pre-frontier intelligence picture.

2) Relationship between ESP and CPIP

The ESP sets out the overall picture of the situation at the external borders, based on information provided by the NCCs and the Agency. It includes information from the NSPs and the common application of surveillance tools. The CPIP relates to information and intelligence on the areas beyond the external borders. Emphasis is placed on the provision of services, including predictive analytical services, covering maritime areas and third countries of origin and transit. The two pictures are combined and thereby provide geographical continuity. Both pictures are shared among the Member States and available to the Agency.

3) Relationship between the NSP and the ESP/CPIP

The content of the NSP and the ESP/CPIP may partially overlap, as parts of the NSPs made available to the Agency and other Member States are also inherent elements in the ESP/CPIP. The relevant provisions of Regulation (EU) No 1052/2013 (e.g. limitations on sharing personal data)[35] apply to all information from the NSPs that becomes part of the ESP/CPIP.

All information contained in the NSP that is not made available to the Agency is handled in line with the provisions regulating the NSPs. These provisions also apply to exchanges of information between two or more neighbouring Member States, as long as of the exchanges do not involve the Agency. The provisions regulating the ESP/CPIP apply automatically whenever the Agency is involved.

The information exchange between these three pictures follows their three common layers.

1) The *events layer* consists of

- incidents on unauthorised border crossings, including information available to the NCC on incidents relating to a risk to the lives of migrants, and on cross-border crime;
- information on crisis situations;
- information on unidentified and suspect vehicles, vessels and other craft and persons present at, along or in the proximity of the external borders, and
- any other event which may have a significant impact on external border control.

[34] Articles 8 to 11 of Regulation (EU) No 1052/2013
[35] Article 13 of Regulation (EU) No 1052/2013

2) The *operational layer* consists of information on own assets and other operational and environmental information.

3) The *analysis layer* consists of general information, analytical reports, intelligence, imagery, geo data and different types of maps.

3.2.2 Ownership and assurance of information and service oriented approach

In principle, information is owned by the node which provided the information (the relevant NCC or the Agency). Ownership can be transferred to another NCC or the Agency, based on mutual agreement. This transfer can take place on case-by-case basis or may be agreed for a particular group or category of information, for example if the information is transferred through an automated link between EUROSUR and other software. The Member State requesting ownership of information is responsible for providing reasons for the request.

The NCCs are responsible for providing as full, accurate and timely a picture as possible. Both the NCCs and the Agency are responsible for ensuring the availability, confidentiality and integrity of the information that has been exchanged. They do this by strictly following the security rules, the rules for protecting classified and personal data and by respecting the ownership rights when further processing information.

The owners of the information are responsible for validating it before publishing it in the EUROSUR communication network (ECN). Efforts must be made to avoid any duplication of information, through appropriate procedures and consistent validation processes. Special attention should be paid to ensuring that information that is manually uploaded does not duplicate information that is already in the system from semi-automated and automated sources (other connected systems). Procedures are drawn up at both Agency and Member State level to minimise this risk.

The Agency takes a service-oriented approach based on internationally agreed standards in delivering information and services to EUROSUR.

3.2.3 Communities of interest[36]

Communities of interest are formed by EUROSUR users that pursue common objectives, requirements or interests. These users can form geographic groups or groups based on subject. For example, a geographic community of interest could focus on a particular area/type of border or on having a common border with a particular third country. A thematic community could focus on further developing the analysis layer or another particular EUROSUR service, or on participating in a joint operation.

These communities are not formally established, but help improve organisation and, in particular, increase cooperation and synergies in service delivery and information exchange, and consequently improve reaction capability. Information exchange and cooperation within these groups is either regulated by NSP or ESP/CPIP provisions, depending on whether the Agency participates.

As they are cross-dimensional, communities of interest may reach beyond the scope of EUROSUR, and separate provisions (e.g. general mandate of the Agency) apply to the parts not covered by EUROSUR. For example, if a group of Member States participating in a joint operation forms a community of interest, part of the information collected and processed by the Agency as part of that operation may be out of scope for EUROSUR (information on return proceedings, asylum, etc).

[36] See Annex to Regulation (EU) No 1052/2013.

3.2.4 Sources of information[37]

Category	Non-exhaustive list of examples
A — National surveillance system	– Land border surveillance system(s) – Maritime surveillance system(s) – Air border surveillance system(s)
B — Fixed and mobile sensors	– Radar: position, course, speed, time, size of target – Cameras: pictures, videos, time, direction, image-processed data – Active range gated cameras: target distance, ship identification – Radio frequency sensors/direction systems: position, operating frequency, radio type – Hydrophone systems: ship movement data, ship identification
C — Patrols	– Sea, land and air border surveillance missions – Military assets assisting a law enforcement mission – Search and rescue missions – Customs/fishery control missions – Maritime safety missions (e.g. oil spill detection)
D — Local, regional and other centres	– Local and regional coordination centres – Maritime rescue coordination centres
E — Other authorities and systems, including liaison officers	– National contact points for the prevention of illegal immigration/drug smuggling – Operational centres for cross-border cooperation – National centres for fishery control/for maritime safety and security – Contact points between neighbouring Member States (e.g. for false documents. borders. customs. or tackling cross-border vehicle crime) – Embassies, consulates and liaison officers in third countries
F — the Agency	– EUROSUR Fusion Services including information from the common application of surveillance tools (e.g. vessel detection service, satellite imagery, terrain information, weather forecast) – Analytical products developed by the Agency's risk analysis unit (e.g. impact levels allocated to border sections) – Joint operation information, including event reports sent through the *joint operations reporting application* (JORA) – Information on the Agency's own assets
G — Other NCCs	– Neighbouring border sections: incidents, tactical risk analysis reports and, possibly, patrols – Regional networks – European patrols network (EPN)
H — Third countries	– Regional networks – Bilateral cooperation
I — Ship reporting systems	– Automatic identification system (AIS) – Vessel monitoring system (VMS) – Union Maritime Information and Exchange System, including SafeSeaNet (SSN) and the Long-range identification and tracking system (LRIT)

[37] Article 9(2) of Regulation (EU) No 1052/2013.

3.2.5 Events layer[38]

For land and sea border surveillance Member States must report all events as set out in the following chapters, regardless of the impact level of the given event.

If a Member State decides to report incidents at border crossing points or incidents relating to air border surveillance, it should:

- declare the scope of this reporting to the Agency; and
- fully adhere to the declared scope when reporting.

Issues related to border checks and air border surveillance are relevant for developing full situational awareness. Member States should therefore continue to provide information on these once they have started and stop doing so only in exceptional and duly justified cases. If they stop reporting, Member States must declare the cessation of reporting to the Agency.

3.2.5.1 Form of NSP events layer

The sub-layers of the events layer are not to be understood as physically separated, but as information sets relating to different subjects, which can be displayed in various ways, with the objective of improving situational awareness and reaction capability in the most effective way. The way events are collected in the NSP should allow the easy transfer of all events to the ESP without delay, e.g. by semi-automated/automated interface transfer or swift manual insertion of those events to the ESP.

3.2.5.2 Sub-layer on unauthorised border crossings

All incidents relating to unauthorised border crossings detected at the external borders of the Member State must be reported in the NSP, regardless the number of people involved, their nationality, or the impact level of the incident. It is best practice to also include incidents related to border checks and air border surveillance to achieve full situational awareness.

3.2.5.3 Sub-layer on cross-border crime

This sub-layer refers to any incidents relating to serious crime with a cross-border dimension that take place at, along, or in the proximity of the external borders.

3.2.5.4 Sub-layer on crisis situations

This sub-layer covers natural or man-made disasters, accidents, humanitarian or political crises or any other serious situations occurring at, along, or in the proximity of the external borders that may have a significant impact on border control. Significant impact, in this context, is to be understood as affecting conditions at the border to such an extent that additional measures or special intervention need to be taken, including the need for reinforcements and urgent decision-making and response.

3.2.5.5 Sub-layer on other events

This sub-layer contains information on unidentified and suspect vehicles, vessels and other craft and persons present at, along, or in the proximity of the external borders of the relevant Member State, and any other event which may have a significant impact on the control of the external borders.

[38] See Articles 4(2) and (3), 9(3) and (4), 10(3) and 11(4) of Regulation (EU) No 1052/2013.

3.2.5.6 NSP events layer elements to be shared with the ESP

All events reported in the NSP must also be made available in the ESP. The NCC must ensure that they are uploaded and forwarded to the ESP without delay.

3.2.5.7 Border sections assignment

All events are assigned to a border section.

3.2.5.8 Impact level for incidents

When maintaining their respective NSPs, NCCs allocate an impact level, based on a national assessment, to all events it reports. The Agency cannot change the incident impact levels that the NCCs have allocated.

3.2.5.9 Events layer of the ESP/CPIP

The ESP and the CPIP are available to all Member States participating in EUROSUR. The Agency must give the NCC, via the ECN, unlimited access to both pictures.

The contents of the CPIP mirrors the structure presented in the ESP, which means the information covers the same thematic areas. Together, the CPIP and the ESP provide geographic continuity. There may be incidents which are detected in the area covered by the CPIP and intercepted in the area covered by the ESP.

All events taking place in the operational area of a joint operation, pilot project or rapid intervention coordinated by the Agency must be reported in the ESP/CPIP, including those that took place in the operational area but not as part of the joint operation itself. European patrols network operational areas and any other operational activities that involve the Agency fall into this category.

3.2.5.10 Reporting process and quality assurance

Member States and the Agency must ensure that reporting is of an appropriate quality and that there is no duplication of reporting (e.g. of incidents) in the EUROSUR framework. To do this, Member States introduce a validation mechanism, which makes the NCC responsible for the final validation of data provided to the ESP/CPIP. The NCC must also ensure that no personal data other than those concerning ship identification numbers is uploaded to the ESP/CPIP.

The national Frontex point of contact (NFPOC) informs the NCC in advance about any operations planned that will take place on its territory.

3.2.6 Operational layer[39]

3.2.6.1 NSP

The operational layer consists of:

- a sub-layer on own assets and operational areas; and
- a sub-layer on environmental information (see chapter 3.2.6.5).

The sub-layer on own assets and operational areas contains information on national assets and personnel, as defined and maintained nationally.

Information on own assets and operational areas is collected in national systems of Member States. This may include, for example, a visualisation of the areas of responsibility of

[39] See Articles 9(5) and (6), 9(9) and (10, 10(5) and (6) and 11(4) of Regulation (EU) No 1052/2013.

subordinate structures on a geo-referenced map, the position and itinerary of patrols, the distribution and type of assets, real-time images provided by video cameras, the area covered by cameras and the position and coordinates of patrol vessels on rivers and the sea. Direct communication between the NCC and patrol assets via specific terminals (e.g. Trans-European Trunked Radio/TETRA) considerably improves reaction capability.

Information on military assets assisting a law enforcement mission may be restricted on a need-to-know basis at the request of the national authority responsible for such assets.

Interlinking information provided in the operational layer (e.g. on patrol assets and weather conditions) with information from the events layer considerably improves situational awareness and reaction capability.

The situational picture of neighbouring external border sections contained in the operational layer may be shared between the Member States involved and may also be shared with the Agency on a voluntary basis.

3.2.6.2 ESP/CPIP

This layer consists of:

- a sub-layer on own assets;
- a sub-layer on operations; and
- a sub-layer on environmental information (see chapter 3.2.6.5).

The sub-layers on own assets and on operations contain information provided by the Member States and by the Agency, where the assets participate in the Agency's joint operations or are at the disposal of the Agency. The following information is required for all *assets* taking part in operational activities coordinated by the Agency:

- type of asset
- name of asset (brand/model/call sign)
- description (detailed asset type indication)
- owner — referring to Member State (standard description, including the three-letter country code (ISO 3166-1 alpha-3 standard) of the deploying Member State authority)
- location (last deployment base)
- name of the operation

Furthermore information is included about the assets' status and position (e.g. an asset participating in a joint operation sends the information on its position through the Frontex positioning system), mission statement and involved actors, deployment and patrolling schedules, operational areas, periodic situational reports, statistical information, focal and coordination points and about other operational activities coordinated by the Agency, such as the European patrols network (EPN).

Best practice is that the NCCs host activities coordinated by the Agency, including the International Coordination Centre (ICC). Where the ICC is separate from the NCC, proper communication channels and procedures must be put in place for information exchange between them on activities coordinated by the Agency.

3.2.6.3 European patrols network (EPN)

All EPN Member States use the EUROSUR framework for sharing EPN information. EPN Member States use their NCC and the ECN to

- report all *incidents* relating to illegal immigration and cross-border crime encountered in EPN areas to the events layer of the ESP/CPIP. Standard mission reports, videos and images can be attached to provide details of the incident, if available;
- provide information on EPN *common patrols* to the operational layer of the ESP/CPIP, including information on observers (such as liaison officers) on-board patrolling assets;
- verify and update the *EPN areas*[40] in the operational layer of the ESP/CPIP; and
- update information on key elements (e.g. EPN patrolling schedules and monthly information on patrols carried out in EPN areas, changes in EPN structures).

Information relating to day-to-day cooperation among EPN Member States needs to be clearly marked in the operational layer of the ESP/CPIP.

3.2.6.4 Roles and responsibilities

Information about operations, pilot projects and rapid interventions coordinated by the Agency should be provided as follows:

- The Agency will insert information on the operational area for joint operations.
- The host Member State will provide information on the assets participating in joint operations, but this may also be provided by the Agency upon agreement with the host Member State.
- The Frontex positioning system provides the position, time, status and type of assets participating in joint operations**,** pilot projects and rapid interventions or which are at the disposal of the Agency. If the assets participating in the joint operation are not connected to the Frontex positioning system, the NCC of the Member State hosting the joint operation must provide a frequent update of the number, position and status of the assets deployed.

The Agency may also share via the operational layer of the ESP/CPIP other information about operations, pilot projects and rapid interventions coordinated by the Agency, such as:

- daily/weekly situational reports for each specific joint operation;
- tailored information for media purposes.

3.2.6.5 Sub-layer on environmental information

This sub-layer gives access to information on terrain and weather conditions. The Agency provides via the operational layer of the ESP/CPIP weather observations, weather forecasts, oceanographic information and drifting model services, which may be also used for the NSP.

3.2.7 Analysis layer[41]

The analysis layers of the ESP/CPIP and NSP are interlinked, as they may be based on the same situational and intelligence data. The two tables below contain the product and service types that are the same in the analysis layer of both the NSP and the ESP/CPIP.

Analysis layer products are, by default, not delivered on demand but provided based on specific internal NCC or Agency taskings.

[40] These areas have been established based on Member States' patrolling activities, covering specific coastal areas of the Mediterranean Sea, the Atlantic Ocean and the Black Sea.
[41] See Articles 9(7), 10(7) and 11(4) of Regulation (EU) No 1052/2013.

Products	Description
Key developments	Brief report containing a concise description and analysis of events or political, social, economic or demographic conditions, including the fundamental rights situation, which have or could have an impact on illegal immigration or cross-border crime.
Briefing note	A concise and usually ad hoc report analysing specific illegal immigration or cross-border crime issues. Its main purpose is to quickly and effectively inform decision-makers about a specific issue.
Analytical monitor	A regular and more detailed report (in comparison to the briefing note) on illegal immigration or cross-border crime, covering specific regions or issues. It goes further than a briefing note, providing a more in-depth analysis of the situation and, if possible, recommendations.
Earth observation reports	Reports delivered by the EU Satellite Centre or enterprises in response to requests for earth observation services such as coastal monitoring or pre-frontier monitoring.
Supporting analytical reports	This category is meant to allow analytical documentation that do not fit into the main analysis layer products types (key developments, briefing notes and analytical monitors) to be shared through EUROSUR.

Analysis layer services are all 'on demand' services, which NCCs can requested through *EUROSUR Fusion Services* (see chapter 3.2.8). By default, these services will be shared will all NCCs through the ECN.

Services	Description
Coastal monitoring	Punctual and ad hoc reports, vectorised data and imagery of coastal strips (beaches and ports) chosen through risk analysis. These support the operational assessment of illegal immigration and cross-border crime related activities.
Pre-frontier monitoring	Punctual and ad hoc reports, vectorised data and imagery of the pre-frontier area chosen through risk analysis. These reports support the operational assessment of illegal immigration and cross-border crime related activities. This service allows for border permeability studies to be requested.
Reference imagery / mapping	Very high resolution satellite imagery and vectorised data covering specific third-country areas chosen through risk analysis. This imagery is required for current and future analysis of illegal immigration and cross-border crime related activities.

The following seven steps are used for to generate and manage the analysis layer:

- Step 1: management of the analysis layer
- Step 2: intelligence collection
- Step 3: intelligence evaluation
- Step 4: intelligence collation
- Step 5: analysis and interpretation
- Step 6: generation and visualisation of products and services
- Step 7: dissemination

3.2.7.1 Step 1: management of the analysis layer

This overarching task aims to manage the analysis layer and the associated intelligence cycle. It is achieved through identifying or improving tasks, procedures and policies.

3.2.7.2 Step 2: intelligence collection

The Agency collects information and intelligence based on agreed requirements, focusing on a target, pattern or trend. Collection involves gathering information from multiple sources in different formats, initially mostly from outside EUROSUR (joint operations, liaison officer and risk analysis networks, EU agencies, missions and delegations, or UN agencies, funds and programmes). This gradually changes, depending on the quantity and quality of NCC intelligence contributions to EUROSUR. This step captures the types of information and intelligence required to generate the ESP/CPIP analysis layer:

- *Imagery and geo-data:* spatially referenced information like topographic maps, transport infrastructure, nautical charts, restricted areas, thematic maps and digital elevation models, including reference imagery for key illegal immigration areas and locations identified by analysis and intelligence.
- *Strategic key information:* covering long-term reviews, emerging trends and changes in combating illegal immigration and cross-border crime, possible mitigation and prevention measures and likely avenues for changes to policies, programmes and legislation.
- *Operational information:* Tactical and operational information such as sensor data, vessel detection and tracking, radar imagery, patrol assets, incident reports, satellite imagery, operational intelligence and surveillance information (signals intelligence, human intelligence).
- *Knowledge base data:* The knowledge base will contain a formalised description of terms and methods such as the categorisation of vessel types, descriptions of typical scenarios, and sensor descriptions. It will provide a means for manual and semi-automatic collection, organisation, and retrieval of knowledge.

3.2.7.3 Step 3: intelligence evaluation

This step consists of two tasks:

- *Evaluation:* assessment of the reliability of the source and credibility of the information;
- *Validation:* assessment of incoming filtered data against standardised criteria (including legal checks), to improve data quality.

3.2.7.4 Step 4: intelligence collation

Collation involves the sifting out of spurious, non-relevant, and incorrect information. It requires arranging the remaining information, allowing the identification of any relationships between apparently disconnected elements. It includes two tasks:

- *Filtering:* suppressing information that is not essential to immediate information requirements;
- *Fusion:* merging evaluated and validated information into a single, coherent deliverable.

3.2.7.5 Step 5: analysis and interpretation

The analytical step converts information into an interpreted product that provides the most precise and valid forward-looking inference possible.

- *Tactical/operational intelligence* contributes directly to an immediate objective and is focused on, for example, specific criminal activities with the goal of neutralising them.

– *Strategic intelligence* deals with existing patterns or emerging trends of illegal immigration and cross-border crime activities. Its goal is achieved through synthesising and analysing data collected over a period of time in order to produce informed judgments about issues such as facilitation capabilities, vulnerabilities, trends and patterns. It allows for conclusions and forecasts to be produced which will assist in developing appropriate countermeasures.

– *Imagery analysis* is a key information-, target- and strategic intelligence-generating activity, based on satellite imagery exploitation. It detects and analyses changes, and allows for correlation/fusion with other sources (open source, geospatial, strategic development information and third party sources), analytical reports and other supporting materials.

Analyses are tailored to customer needs to effectively assist the decision-making process.

3.2.7.6 Step 6: generation and visualisation of services and products, and Step 7: dissemination

In these steps, the outputs of the analysis and interpretation step are corrected, condensed, organised, and modified, prior to the publication of documents and display of objects and maps. The final phase is the upload of all new and updated analysis layer products to the NSP or the ESP/CPIP. Once products are able to be seen in the ESP/CPIP, they are considered to have been disseminated.

3.2.8 Common application of surveillance tools[42]

3.2.8.1 The Agency's role

The Agency coordinates the common application of surveillance tools at European level by providing centralised services to Member States and the Agency. As coordinator, the Agency must be the single point of entry/exit for the acquisition, fusion and delivery of these services.

3.2.8.2 Service activation

Services are activated based on *the requirements* for maintaining the ESP and the CPIP, *a request* from the NCC *a request* from the Agency's units (e.g. to support joint operations).

3.2.8.3 Service delivery

1) Scope of services: The table below shows the scope of services that may be provided:

Service scope	Regulation (EU) No 1052/2013	Provision
Environmental information including: - terrain information (e.g. base maps) - weather conditions	10 (5) (c)	Regular
Coastal monitoring	12 (2) (a)	On request
Tracking of vessels	12 (2) (b)	On request
Monitoring of designated maritime areas	12 (2) (c)	On request
Environmental assessment of designated areas	12 (2) (d)	On request
Pre-frontier monitoring	12 (2) (e)	On request
Ship reporting systems data	12 (3) (a)	Regular

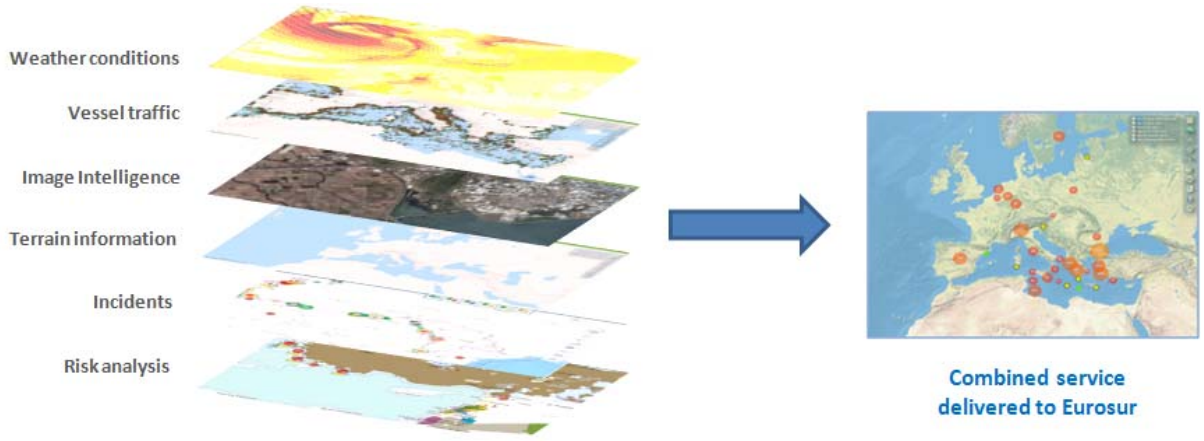
[42] Article 12 of Regulation (EU) No 1052/2013.

2) Fusion of services

Under the *EUROSUR Fusion Services* framework, the Agency acquires, combines and displays basic and combined services from different surveillance tools and other sources in the ESP/CPIP customised to meet the needs of the end user. Whenever necessary, services may be enriched by providing appropriate risk analysis.

Examples:
- incident detection time service;
- maritime models, such as drifting models (allowing for the calculation of probable locations of vessels, based on the last position and sea conditions);
- anomaly detection (allowing the detection of suspicious or atypical behaviour by vessels);
- vessel traffic service, including combining vessel positions acquired via the automatic identification system (AIS) and satellite AIS with data on vessel positions recorded by terrestrial and satellite radars.

The illustration below shows a combination of different and separated services provided by internal and external suppliers into one single, combined service.



3) List of services

The Agency will provide services either on a regular basis or on an ad hoc basis, depending on needs. The Agency makes available to NCCs a list of services, which contains information and details of each of the services provided on a standard basis. If a need is identified, a new service, not previously included in the list, may be provided.

4) Service process

The Agency uses a service delivery process cycle that begins when a request is made and ends when the service is activated. The process includes all the steps to ensure:

– the necessary assessment and validation of the service request against a set of predefined criteria;

– appropriate workflows for delivering standard services and designing and developing new services; and

– delivery of the service to the user.

5) Validation criteria

The Agency assesses and validates each service request before the service is provided. It may either agree to deliver the service or refuse the request for technical, financial or operational

reasons. If it refuses the request, the Agency informs the relevant NCC and provides an explanation for the refusal.

3.2.9 Personal data policy[43]

3.2.9.1 NSP[44]

Member States process personal data in the NSP in accordance with their national provisions. Every Member State which processes any personal data in their NSP is responsible, in particular, for the security of this data, appropriate training of staff and compliance with national data protection rules and requirements.

Member States make sure that, upon expiry of the data retention period set under national law, personal data is deleted or anonymised according to national law. Whenever the NSP includes personal data, processing of such data should be logged to provide an audit trail.

3.2.9.2 ESP and CPIP[45]

The NCC must ensure that no personal data other than data relating to ship identification numbers is uploaded to the ESP/CPIP. To avoid the risk of unintentionally uploading personal data to the ESP/CPIP, Member States should create a validation mechanism at NCC level to check that no personal data is included in information forwarded to the ESP/CPIP when it leaves the NSP. This validation mechanism may consist of:

- avoiding using cut and paste from national databases, if these include personal data;
- reading inserted text, especially free text fields, a final time before sending, while paying specific attention as to whether personal data have been inserted;
- requiring users to pay attention to the content of documents that they attach to artefacts, and to the content of stand-alone documents, because these could include personal data.

Mechanisms in the EUROSUR communication network (ECN) should ensure that data stored in the NSP which is tagged as personal data by the information owner (e.g. the NCC) is not shared with any other NCC except for personal data allowed in the ESP/CPIP.

If the Agency encounters personal data other than data relating to ship identification numbers in the ESP/CPIP, it must notify the owner/originator of the data (e.g. the NCC) and request the removal of that data. The owner of the data must delete it from the ESP/CPIP.

The Agency cooperates with the European Data Protection Supervisor (EDPS) on this issue.

3.2.9.3 Bilateral exchange between neighbouring Member States[46]

If neighbouring Member States use the ECN for the bilateral exchange of information, personal data must be excluded. This does not prevent Member States from bilaterally exchanging personal data through specific communication lines in accordance with national and EU data protection rules.

[43] Article 13 of Regulation (EU) No 1052/2013.
[44] Article 13(1) of Regulation (EU) No 1052/2013.
[45] Article 13(2) of Regulation (EU) No 1052/2013.
[46] See Article 9(9) and (10) of Regulation (EU) No 1052/2013.

3.3 Reaction capability[47]

3.3.1 Definition and components

Reaction capability means the ability to perform actions aimed at countering illegal cross-border activities at, along, or in the proximity of the external borders, including the means and time to react appropriately. At the same time it is one of the key factors contributing to protecting and saving migrants' lives. National authorities with responsibility for external border surveillance need to be able to re-allocate resources, such as staff, equipment and assets to quickly react to any changes at sea and land external borders and, if applicable, at border crossing points.

Reaction capability has two components:

- *Physical reaction capability* is the availability of sufficient human and technical resources (such as trained personnel, systems and assets), which allows for an appropriate reaction to sudden threats or illegal activities.

  Recommendation: monitor external border sections with stationary and mobile equipment that at least meet the requirements for low impact level sections.

- *Procedural reaction capability* refers to the existence of processes and procedures enabling authorities to plan, initiate and conduct operations to counter threats or illegal cross-border activities efficiently and rapidly.

  Recommendation: for all external border sections, even for those with consistently low impact levels, a procedure or mechanism for activating additional resources is in place, in case of sudden threats or a sudden increase in the impact level.

3.3.2 Reaction capability planning

The NCCs organise and carry out *simulations* of possible scenarios and evaluate the appropriate reaction measures. This will allow them to

- define, structure and coordinate the relevant reaction measures by the national authorities responsible for border surveillance at the different external border sections and support measures provided by other national authorities;
- assess the overall reaction capability and identify any need to further improvement.

Recommendation: Plans should be drafted on coping with sudden mass influxes of third country nationals.

Reaction capability planning can be divided into measures done at local, regional, national and international level. As far as possible, the NCC should be used as a coordination and information exchange body. If a Member State already has such plans, it checks whether they meet the requirements of this handbook and, if necessary, adjust them accordingly.

Best practice: Reaction capability planning can cover for each border section:

- description of the external border section (terrain, geopolitical, environmental) and risk analysis overview;
- resources available in national authorities responsible for border surveillance and in supporting authorities (human and technical resources, their location, quantity, response time, communication channels);

[47] See Articles 14 to 17 of Regulation (EU) No 1052/2013.

- authorities in neighbouring Member State(s) external border sections and their resources;
- authorities in neighbouring third countries' border sections and their resources;
- rules of engagement on jointly agreed reaction to different scenarios;
- provisions regarding the mechanisms to protect fundamental rights, including international protection and the protection of vulnerable groups in case of mass arrivals;

The reaction capability needs to be adaptable to changing situations.

Recommendation: Reaction capability should be planned separately for low, medium and high impact levels allocated to the external border sections, including a description of measures to be taken if the impact level allocated to an external border sections changes. The plans should also include the deployment of national rapid intervention teams and the Agency's support activities and resources.

3.3.3 Delegation of tasks to regional and local levels[48]

Member States may delegate some of the NCC's responsibilities to regional, local, functional or other authorities that are in a position to take operational decisions ensuring reaction capability in their respective areas of responsibility. This allocation of tasks must not affect the NCC's role as the single point of contact for cooperating and exchanging information with other NCCs and the Agency.

3.3.4 Border sections

Each Member State must divide its external land and sea borders into border sections and notify the Agency of these.[49] They must also notify the Agency of any changes in this regard.

The area covered by a border section corresponds to the area of responsibility for a local or regional centre, ensuring the efficient management of personnel and resources.

At the Agency's request, Member States provide the Agency with the information from the:

- border sections and border crossing points;
- border sections' characterisation;
- border sections' thresholds.

The Agency must assign a unique identifier to all newly created border sections and then include them on the EUROSUR border sections list.

3.3.5 Border sections' impact levels

When assessing the EUROSUR impact levels, the three components of risk (threat, vulnerability and impact) must be taken into account, using the CIRAM model for risk analysis developed by the Agency:

1) the threat must be assessed in terms of impact and likelihood;
2) the vulnerability to the threat: level and efficiency of response to the threat;
3) the impact: should the threat occur.

[48] Article 17 of Regulation (EU) No 1052/2013.

[49] Border sections, as defined by a Member State, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries, or to the name of any territory, city or area.

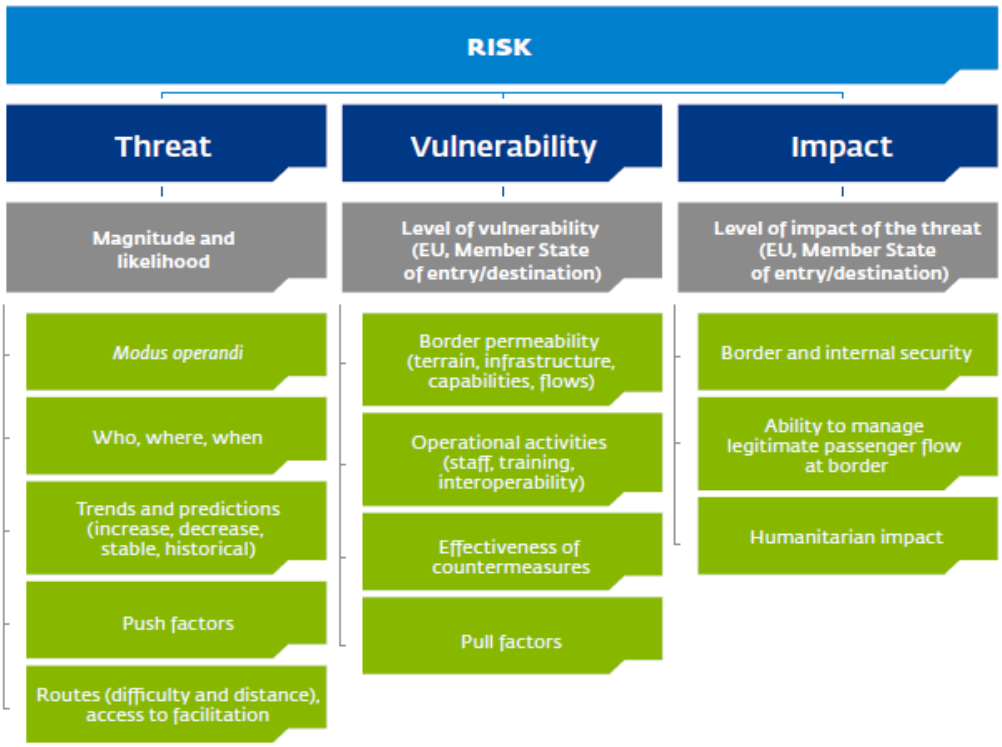


Table: Risk components (CIRAM)

3.3.5.1 The Agency's impact level assessment

The Agency must assess EUROSUR impact levels on a regular basis.

The Agency will evaluate variables describing the threats following the CIRAM model. Sets of variables are assessed to identify the level of threat for each border section, focusing on the key developments affecting the *threat level*. The main factors are:

1. Statistical trends which describe the numerical trends related to illegal land and sea border crossings, taking into account the historical baseline compared to the current situation.
2. Geopolitical and natural push factors that facilitate cross-border criminal activities or motivate would-be migrants to leave their country of origin/transit. Countries of origin and transit should be differentiated.
3. Factors affecting cross-border crime and the movement of migrants in countries of origin and transit along the route towards Member States.
4. Facilitation analysis, including assessing activities and characteristics of facilitation networks along transit routes and within the most recent departure countries.

The main factors to be taken into consideration while assessing the *vulnerability level* are:

1. the assessment of pull factors for the countries of destination and countries of transit;
2. the capacity of border control authorities / border permeability;
3. EU and national policies in the field of migration and law enforcement;
4. the capacity of the authorities to fight criminal networks.

CIRAM *impact factors* will also be assessed, including:

1. humanitarian needs and fundamental right issues;
2. issues impacting on public security and border control.

3.3.5.2 Changes to border sections' impact levels

The impact level of any border section can be updated at any time. A request to update an impact level can come from the relevant Member State(s), which is transmitted via the NCC, or from the Agency. As a general rule, the impact level is updated when the Member States and the Agency agree to do so.

The Agency reviews and revises the impact levels regularly and also on an ad hoc basis.

3.3.5.3 Deadlines

NCCs and the Agency have a deadline for initial responses to requests for impact level changes. Tacit approval is given in those cases where no response has been received from the NCC or the Agency by this deadline. When this happens, the impact levels recommended by the NCC or the Agency will be allocated and included in the ESP. In such cases, the impact levels are allocated with a caveat clearly indicating the tacit nature of the approval.

If the initial response to the request for change is negative, then a bilateral agreement is sought, until the expiry of a second deadline. If, following these discussions, agreement cannot be reached on allocating an impact level to a specific border section, then the Agency's recommended impact levels will be allocated and included in the ESP. In such cases, the impact levels are allocated with a caveat clearly indicating the dissenting position.

These deadlines have been introduced to ensure that changes to the impact levels are made within a reasonable and harmonised timeframe, ensuring the standardised allocation of impact levels.

3.3.6 Reactions depending on impact levels[50]

Member States are primarily responsible for ensuring an appropriate reaction to the situation at the external borders. They must make sure that the border surveillance activities carried out at the external border sections are appropriate to the impact levels allocated. If there are rapid and/or unexpected changes to the situation, Member States must ensure an appropriate reaction.

3.3.6.1 Roles of coordination centres

Member States may, depending on their internal division of responsibilities, structure their national border surveillance activities as follows:

The *local coordination centre* (LCC) responsible for a land or sea border section carries out the following tasks:

- providing guidance at local level;
- carrying out detailed planning and implementation of operations;
- collecting and processing information needed to implement operations;
- organising regular surveillance on the basis of risk analysis;
- ensuring that sufficient personnel and resources are being kept at the border section in readiness for tracking, identification and interception;
- choosing the actions to take in close-to-real time to execute the operation;
- requesting support from the regional/national coordination centre;

[50] Article 16 of Regulation (EU) No 1052/2013.

- ensuring that the patrol or the LCC pass on information about all incidents in the external border section to the NCC in near-real time;
- ensuring that information on all search and rescue incidents at the external border section is communicated by the patrol directly and as a matter of priority to the Maritime Rescue Coordination Centre (MRCC) and to the emergency services;
- if a medium or high impact level has been attributed to a border section, the LCC provides the NCC and the RCC with a weekly report on the measures taken.

Best practice:

Direct and secure communication lines between the LCC and the patrols operating in the border section are established.

The LCC has sufficient resources and personnel at its disposal to ensure regular surveillance on the basis of risk analysis. Additional resources and personnel have been identified that can be made available if the impact level for a border section is raised to medium or high.

The *regional coordination centre (RCC) or other functional coordination centre* covers one type of border section (e.g. land or sea), several border sections in one geographical area or a specific task in all border sections (e.g. customs control, search and rescue). They carry out the following tasks:

- providing guidance at regional/functional level;
- monitoring the planning and implementation of operations;
- collecting and processing information needed to plan operations;
- ensuring that appropriate surveillance measures are being taken at each border section and notifying the NCC on measures taken and the results of these;
- redistributing resources and personnel (.e.g. between border sections);
- requesting support from the NCC;
- ensuring that the patrol or the LCC pass on information on all incidents at the external border section in a timely manner to the relevant national authority's command and control centre (if available), and to the ICC wherever applicable, by putting in place an appropriate reporting mechanism;
- summarizing and analysing for the NCC the information received from the LCCs;
- if a *medium* impact level has been allocated to a border section, ensuring that the relevant LCC receives appropriate additional resources and personnel within *two weeks*.

Best practice: Workflows to swiftly redistribute resources and personnel between border sections are set out, including the workflow needed if the RCC or functional coordination centre needs to request assistance from the NCC.

The *national coordination centre (NCC)*, which is responsible for all border sections, carries out the following tasks:

- providing guidance at national level;
- agreeing working and liaison arrangements with relevant national authorities, where appropriate;

- supporting the overall planning of national operations and monitoring their efficient implementation;
- processing information and risk analysis needed to support the planning of operations;
- coordinating support given at national level (e.g. from different national authorities);
- ensuring that the NCC forwards information on all incidents occurring at the external borders to the Agency no later than *four hours* after having received it from the LCC;
- if a *high* impact level has been allocated to a border section, the NCC
- ensures that the relevant LCC receives appropriate additional resources and personnel within *three weeks*;
- requests support from the Agency; the Agency replies (positively or negatively) to a request for support from the NCC within *five* working days, identifying timelines and the scale of potential support;
- regularly informs the Agency of the measures taken (preferably on a daily basis) and provides the Agency every month with a summary report about the measures taken.[51] The Agency will use these reports in their regular border section assessment.

Best practice:

Direct and secure communication lines between NCC and RCCs/functional coordination centres/LCCs and other relevant national authorities are established.

Rules for workflow, exchanging classified and unclassified information and day-to-day cooperation between the NCC and RCCs/LCCs are set out.

The NCC has an overview of resources and personnel deployed in each border section and an overview of additional resources and personnel available at national level, which could be provided to border sections with a high impact level.

Where different impact levels have been allocated to neighbouring external border sections, the Member State(s) involved may determine potentially critical areas within the border section and dedicate additional resources for border surveillance to this area.

3.3.6.2 Low impact level

For border sections with a low impact level, the Member State must keep sufficient resources in the border area. At regional and local level, reserve resources must be identified and used on request.

3.3.6.3 Medium impact level

If a medium impact level has been allocated to an external border section, the Member State must, in addition to the activities described above, increase the level of surveillance by implementing additional measures. Member States must use risk analysis and available surveillance tools as inputs to their activities. The NCC must be notified if any such surveillance measures are taken. The NCC may grant support, either on request or on its own initiative, to reinforce resources at that border section.

Best practice: At strategic level, the NCC provides situation monitoring, risk analysis and input into the management of resources and personnel, including planning of reserves.

[51] The NCC may combine with this reporting with the ICC reporting whenever appropriate.

At operational and tactical level, the RCC and LCC implement the additional surveillance measures and carry out intensified border control activities, especially in areas identified as critical within the border section.

3.3.6.4 4.5.6.4. High impact level

If a high impact level is allocated to an external border section, the Member State must ensure that stronger surveillance measures are taken at national level.

Best practice: The NCC:

- designates an officer responsible for monitoring and managing the situation at the respective external border section;
- is provided with reinforcements in order manage the increased need for information exchange, risk analysis and cooperation at national level and with neighbouring countries;
- launches, if needed, the emergency task force consisting of all involved authorities;
- manages the involvement of other national authorities;
- assesses the situation and, if needed, request support from the Agency.
- The local/regional level:
- deploys additional resources under the coordination of the leading national authority;
- keeps the NCC informed about any measures taken and their impact.

The Agency has separate procedures to provide the support listed above. If justified, the Agency has the right to refuse requests for support on a case-by-case basis.

3.3.7 Cooperation with neighbouring countries

Where a medium or high impact level is allocated to an external border section adjacent to another Member State or of a country with which it has agreements or regional networks, the NCC contacts the neighbouring country and coordinates the necessary cross-border measures. Member States must also make efforts to strengthen cooperation with third countries with whom they share a border to which a high or medium impact level has been allocated.

Coordination among neighbouring countries must be based on relevant bilateral agreements that comply with norms and standards equivalent to those set by EU and international law. If possible, the NCC should make other NCCs aware of the existence of such agreements, so that other Member States can ask the NCC to facilitate information exchange with this third country, in case of operational need. Potential ways to strengthen coordination between neighbouring countries include:

- agreeing on a common language and terminology;
- setting up information exchange mechanisms;
- exchanging situational pictures of border sections of neighbouring Member States;
- carrying out joint activities on a regular basis — e.g. common patrolling and joint operations of Member States;
- setting up common procedures to help work together in specific scenarios.

3.3.8 Evaluation

In its risk analysis reports, the Agency shall, together with the relevant Member State(s), evaluate the allocation of impact levels and the measures taken as a result at national and EU level. Reaction time is an appropriate measure for assessing reaction capability. At the tactical level, this is the time needed to process an alert, move assets to the hot spot, and prepare to counter the border violation, starting at the moment of detection, and ending when all assets are in place and all operational preparations have been completed.

4 Technical guidelines

4.1 EUROSUR communication network[52]

4.1.1 Roles and responsibilities

The EUROSUR communication network (ECN) has been set up as a network of *nodes* exchanging information. A node is a complete set of hardware and software delivered by the Agency to NCCs, enabling each NCC to share information with other NCCs and with the Agency and access the information services the Agency provides. The ECN is maintained and supported by the *EUROSUR Technical Management Services (EMTS).*

The NCC must supply, maintain and support a link to the internet that serves to connect the node to the ECN. The minimum connection speed required is 10 Mbps. More bandwidth may be required, depending on the type of use and the number of concurrent ECN users in the Member State.

Details of the obligations for the Agency and Member States receiving the node are set out in the Memorandum of Understanding regulating the operational use of the ECN, its technical management and the security baseline to be implemented. The Agency continues to own the ECN hardware and software and is responsible for its maintenance and further development.

The Agency supports users of the nodes through node IT administrators and the EUROSUR technical point of contact in each NCC. The ECN is operational 24/7, with the exception of any maintenance periods.

4.1.2 Application management

The EUROSUR application and services are developed and maintained by the Agency in line with the Memorandum of Understanding. Changes in the application are made following the change management process described in Chapter 4.4. The Agency plans releases and their contents and communicates details of these to all the nodes in advance of release. All nodes are informed about progress on deployment and results. Each application and system within the node and in the ECN must be compliant, as applicable, with the standards set by:

- the Open Geospatial Consortium;
- the Open Web Application Security Project;
- the Open Source Security Testing Methodology Manual.

4.1.3 EUROSUR Technical Management Services

The ETMS are located at the Agency's headquarters. The Agency is responsible for delivering these services to the NCCs. The Agency's main responsibilities in this area are:

1. administering the ECN and system maintenance;
2. developing the ECN's hardware and software, following the change processes described in Chapter 4.4;
3. expanding the ECN into new locations;
4. ensuring the security of the ECN;
5. supporting NCC personnel (the technical point of contact and the IT administrator) and all users at the Agency.

Member States' NCCs can access the ETMS 24/7.

[52] Article 7 of Regulation (EU) No 1052/2013.

The ETMS are:

1) Infrastructure and application(s)

- *Support and troubleshooting*: Helping to resolve ICT incidents and problems that may appear in the ECN and supplying the NCCs with information and advice on EUROSUR applications and infrastructure.
- *User and role management*: Assisting the node IT administrators in the creation, modification and deletion of user accounts, and the assigning of EUROSUR roles to user accounts.
- *Monitoring*: Monitoring system status and system functioning in the IT infrastructure and between the nodes.
- *Updates*: Installing the latest software updates to assure that any vulnerabilities or bugs are addressed with the new versions.
- *Backup*: Checking daily backup status in the ETMS infrastructure and the EUROSUR nodes.

2) Security

- *Firewalls:* Event monitoring, troubleshooting, creation, modification and deletion of firewall rules for the whole ECN — with the exception of the firewalls deployed by NCCs.
- *Intrusion prevention system:* Event monitoring, signature and software updates.
- *Virtual private network:* Monitoring, troubleshooting, creation, modification and deletion of site-to-site VPNs between the EUROSUR nodes, and between the EUROSUR nodes and the ETMS infrastructure.
- *Public key infrastructure:* Issuing, revoking and renewing digital certificates, and providing support to the NCC IT administrators when installing the EUROSUR nodes.
- *Security audits:* Conducting periodic security audits (code audit and penetration tests) following the predefined procedures.
- *Documentation:* Creating and updating existing security documentation.

3) Other services

- *Documentation:* Creating and updating technical documentation.
- *Training materials:* Creating and updating training materials and user manuals.
- *Technical training:* Providing technical training for technical personnel in the NCCs and the Agency.
- *Operational training:* Providing operational training for operational personnel in the NCCs and the Agency.

4.1.4 Node IT administrator and corresponding tasks

A Node ICT administrator is responsible in the NCC for providing technical support for the Agency's node, based on the tasks described by the Agency (e.g. creating user accounts), and for carrying out specific technical actions as instructed by the Agency (e.g. restarting services, rebooting equipment) At least one, and preferably two, node ICT administrators are required in each NCC, carrying out the following tasks:

(1) installing certificates received from the Agency;

(2) maintaining the access point to the internet used for the ECN;

(3) managing user access accounts;

(4) managing EUROSUR domain email accounts;

(5) supporting ETMS in tasks that cannot be performed remotely;

(6) requesting support from ETMS for issues that cannot be handled locally;

(7) monitoring the functioning of the national ECN node;

(8) notifying the Agency of dysfunctions and technical incidents;

(9) analysing any technical incidents relating to the ICT system that they have detected or that are the responsibility of the Member State (e.g. a network device in the Member State network is not functioning, making the ECN inaccessible to some users);[53]

(10) reporting issues to the Agency that require the Agency's intervention, or informing the Agency of any issues affecting the link to the internet;

(11) reporting any security issues encountered on the ECN to the NCC informatics security officer and reporting any security issues on the national system connected to the ECN if these may affect the security of the ECN.

4.1.5 Implementation of technical changes

Any change to the ECN or underlying infrastructure that potentially impacts on the ECN or other party's network or on the connections in place, must go through a change management process involving the other party as a stakeholder. Information must be provided in writing to the other party with sufficient advance notice. The change management process must be followed as set out in the Memorandum of Understanding, the ECN security operating procedures and the Agency's internal procedures, in order to maintain a consistent level of security and accreditation.

Every change to the technical environment of the ECN that will affect the availability of the system must be announced beforehand by the Agency (e.g. for changes in the node) or by Member States (e.g. for changes in the internet infrastructure used to establish the VPN links between nodes, or changes in the interconnections). Changes requiring modifications to the other party's system must be announced with sufficient advance notice, taking into account the impact of the change to the other party's system and the estimated time required to study, design and implement these changes.

4.1.6 User manuals

The Agency, via the ETMS, creates, updates and distributes user manuals for the user applications and services available in the ECN. All user manuals must be updated to reflect new developments.

4.2 Training

All EUROSUR users (NCC and Agency staff) must receive adequate training to perform the tasks assigned to them in the EUROSUR framework and thereby ensure the functioning of EUROSUR. The training categories below take into account the different needs of users. The identification and prioritisation of the training needs is an ongoing collaborative process between the Agency and the NCCs. Training needs are compiled in the annual EUROSUR training plan, maintained by the Agency. The organisation of training activities is triggered either by this training plan or on request from users.

[53] This task can be assigned to the NCC ICT support function (e.g. helpdesk) as long as they are able to assess which system has caused the technical incident (i.e. Member State ICT infrastructure or ECN node infrastructure).

Training categories	1. NCC training	2. Technical IT training	3. Application training
Audience	NCC staff (e.g. management, operators, analysts, IT staff)	ECN IT administrators (system administrators, network specialists)	Member States' trainers (training multipliers)
Content	1. Day-to-day routine and crisis management, including compliance with fundamental rights 2. Exchange of experience and best practice 3. Improve NCC cooperation, including staff exchange	1. ECN architecture 2. Maintenance tasks	1. Use of application by different roles (viewer, operator) 2. Management of application for information managers and application managers
Organi-sation and timing	Planned: Periodical for all NCCs On request: At regional/ bilateral level	Planned: Periodical or based on change (e.g. new release/component) On request: E.g. a specific technical problem is identified, or a specific change is required	Planned: Periodical or based on change (e.g. new release, new component)
Provided by:	Selected NCCs hosting the training, in cooperation with the Agency	The Agency	Member States' national trainers and the Agency

Training categories	4. Operational/content training	5. Skills development training	6. Customised training
Audience	Selected users, depending on particular roles and responsibilities	Selected users, depending on particular roles and responsibilities	Selected users, depending on particular roles and responsibilities
Content	Events layer Analysis layer Operational layer Common application of surveillance tools	Content of EUROSUR services (e.g. satellite imagery analysis, fundamental rights, information security training)	Specific need, e.g.: if Member States join EUROSUR; EUROSUR system is interlinked with national systems
Organi-sation and timing	Planned: Periodical or based on change (e.g. new services deployed, new scope of information, new reporting requirements) On request: Following the identification of a specific subject not included in the EUROSUR training plan	Planned: Periodical or based on change (e.g. new services deployed, new scope of information, new reporting requirements) On request: Following the identification of a specific subject which was not included in the EUROSUR training plan	On request: E.g. due to exceptional circumstances
Provided by:	The Agency	The Agency (in cooperation with partners, e.g. EU Satellite Centre)	The Agency in cooperation with partners

4.3 Security policy and security management[54]

4.3.1 Security objectives

The ECN allows the secure handling, storing, transmission and processing of EU classified information (EUCI) up to the level of RESTREINT UE/EU RESTRICTED.

4.3.1.1 Information types

The Agency and the NCCs must ensure that EUCI is appropriately classified, is clearly identified as classified information, and retains its classification level for only as long as necessary. The ECN contains the following types of information:

- classified information: this includes information on assets and all information classified as RESTREINT UE/EU RESTRICTED by the owner;
- sensitive non-classified information: all information which is not classified must be considered as sensitive non-classified;
- personal data relating to ship identification numbers and data tagged by the owner in the NSP as personal data.

Information owners are responsible and accountable for attributing, updating and downgrading classification levels on information. The artefact related to own asset is marked in the ECN as RESTREINT UE/EU RESTRICTED, even if it was not marked as such by the originator. Users cannot declassify these artefacts. The originator of the document must provide prior written consent to downgrade or declassify any other EUCI or to modify or remove any of the markings.

4.3.1.2 Protection of sensitive non-classified and EU RESTRICTED information

The Agency must protect sensitive non-classified and EU classified information in accordance with Article 11(d) of Regulation (EC) No 2007/2004, which requires the Agency to apply the Commission's security rules.[55] All non-classified information handled as part of EUROSUR must be considered 'sensitive non-classified'. In the ECN, this information must be marked, whenever technically possible, as 'LIMITED'.

If NCCs share classified information bearing a national security classification marking with the ECN, the Agency must protect that information in accordance with the requirements applicable to EUCI at the equivalent level, as set out in the table of equivalence of security classifications. NCCs must exchange, process and store non-classified sensitive and classified information in the ECN in accordance with national rules and the security operating procedures set out in the ECN's security accreditation.

4.3.1.3 Personnel security clearance

The criteria for determining whether an individual may be authorised to have access to EUCI take into account his trustworthiness, reliability and loyalty.

4.3.1.4 Granting access to EU classified information — principles

An individual will only be granted access to classified information after:

- s/he has a need to know the information;

[54] See Article 7(3), (4) and (5) of Regulation (EU) No 1052/2013.

[55] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

- s/he has been briefed on the security rules and procedures for protecting EUCI and has acknowledged his/her responsibilities with regard to protecting such information; and
- if national laws and regulations require, s/he has been authorised to access classified information at the relevant level.

4.3.1.5 User access control

Access to the ECN and the ECN application is managed based on the following security principles:

- permissions to access the ECN and the ECN application must be granted based upon individual identification and authentication;
- user access permissions must be restricted based on a 'need-to-know';
- allocation and use of privileged accounts must be minimised;
- ICT systems must be configured to technically enforce this policy;
- user permissions must be reviewed on a regular basis, following a formal review process.

Users will be given access to the ECN following a security process composed at least of inputting and checking a logon name and password, in line with the Agency's standards. This rule also applies to interconnected systems, except for an interconnection through the EUROSUR node integration interface, where national authentication applies.

The Agency and the Member States manage their users by creating, modifying, blocking and deleting their accounts and granting them appropriate access permissions to the ECN to carry out their tasks. To do this, they implement an ECN user management policy to guarantee that the relevant person with responsibility in this area carefully considers the creation of accounts and their associated permissions, based on the user having at least a security clearance or equivalent national authorisation at the 'RESTREINT UE/EU RESTRICTED' level or national equivalent, and on the 'need-to-know' principle. This person carries out an annual review of the ECN's users and their permissions. As a result of that review, s/he makes any changes required to the status of the accounts and their permissions.

Detailed rules and requirements are set out in the accreditation documentation.

4.3.2 Physical security measures

EUCI that is classified as RESTREINT UE/EU RESTRICTED may be handled in 'Administrative Areas'. The Agency and the NCCs must establish that an area meets the requirements before it can be designated as an Administrative Area. This means that:

- a visibly defined perimeter is drawn up, allowing individuals and, where possible, vehicles to be checked;
- unescorted access is granted only to individuals who are duly authorised by the competent authority; and
- all other individuals are escorted at all times or be subject to equivalent controls.

4.3.3 Protection of information handled in communication and information systems

4.3.3.1 Accreditation of the ECN

The ECN and interconnected communication and information systems must undergo an accreditation process as described in the Memorandum of Understanding, signed between the Member States and the Agency. The accreditation process verifies that all appropriate security measures have been implemented and that the EUCI and the communication and information system have been sufficiently protected. The accreditation statement identifies the maximum classification level of the information that may be handled in a particular communication and

information system and the relevant terms and conditions. The accreditation process is managed by the Agency which is the Accreditation Authority, with the support of the Member States and in line with the European Commission's guidelines on the security accreditation of IT systems.

Changes to the system will be made bearing in mind the need to keep the highest possible level of security. This will be done by assessing the risks associated with these changes, identifying and implementing appropriate mitigating measures, and testing the effectiveness of these mitigating measures on a regular basis. Major changes to the ECN may lead to the ECN needing to be fully re-accredited, depending on the result of the risk assessment to measure the impact of the changes on security.

4.3.3.2 Connection of other systems to the network

The ECN may be connected to other systems, as long as the conditions in Article 6 and Annexes 1 and 5 of the Memorandum of Understanding are fulfilled. Accreditation requirements in these cases are set out in the Memorandum of Understanding.

4.3.4 Security roles and responsibilities

4.3.4.1 Security roles within the Agency

Security accreditation authority	The Agency is the security accreditation authority for the ECN. It is responsible for the general area of security and for the specialist areas of information security, communication security and crypto-security.
ECN Security Officer	The Security Officer at the Agency is the ECN Security Officer, responsible for overseeing the overall protection of EUCI.
ECN Central Informatics Security Officer	The Information Security Officer at the Agency is the ECN's Central Informatics Security Officer. S/He is responsible for ensuring that the ECN's security level is maintained at the appropriate level and ensuring that all reported IT incidents are recorded, analysed and solved, in close contact with Member States when needed.
Agency's ICT Security Officer	The Agency's ICT Security Officer is tasked with overseeing the monitoring of the ECN's security aspects and investigating all reported incidents.
Technical Systems Owner	The Technical Systems Owner is responsible for the implementation and operation of checks and special security features in the ECN. S/He specifies the security standards and practices that the system supplier must meet and is responsible for drawing up the security operating procedures.
Data Protection Officer	The Data Protection Officer ensures that personal data in the ECN is handled in accordance with the rules and regulations on protecting personal data that apply to the Agency.

4.3.4.2 Security roles in the Member States

Each Member State will appoint a person to the following roles:

- Person responsible for the organisation of the NCC and physical security measures in the NCC (e.g. Head of NCC). The person assigned to this role must ensure that:
    - physical security measures are in place to protect equipment connected to the ECN and to make sure that only authorised people in the NCC can access this, including (where applicable) people in decentralised offices and all other systems used in the NCC that are connected with the ECN;

- all policies and procedures set out in national standards, national rules and in the Memorandum of Understanding — necessary to protect classified and sensitive non-classified information stored and handled in the ECN or extracted and processed outside it — are implemented in the NCC and applied by the NCC staff (e.g. marking of information or documents, handling of classified documents, overseeing the application of a procedure to assign the right level of permissions to ECN users and review them periodically);
- procedures are put in place, in line with national rules for accreditation (or equivalent procedure), for systems that connect to the ECN; this will require liaison with all relevant national authorities in the Member State.

- The National Coordination Centre's Informatics Security Officer (NCC ISO).

  The NCC ISO monitors security aspects of networks connected to the ECN and investigates all reported incidents. If necessary, the NCC ISO will be supported by the Agency's ICT unit, with the Agency's ICT Security Officer acting as a contact point.

In addition, each Member State must task one of these people with informing the Agency of security incidents that may affect the Agency's ECN node or ECN Technical Management Services and with informing any other Member State(s) affected of any security incidents that may affect their ECN node.

4.3.4.3 Other roles — in both the Agency and Member States

The Information Owner: The Information Owner is responsible for EUCI and other information that is added to, processed in and produced by technical systems.

Users: All users are responsible for applying policies and procedures and for ensuring that their actions do not adversely affect the security of the system that they are using.

4.3.5 Control mechanisms and reporting procedures if there is a security breach

Any behaviour by any component of the ECN or an interconnected system that could suggest that a security incident has occurred or is occurring in the ECN or could be affecting the ECN must immediately be reported to and analysed by the NCC ISO. If his/her analysis confirms that the risk is high, s/he must immediately report the incident to the Agency, in line with the rules and processes set out in the accreditation documentation.

4.4 Change management[56]

4.4.1 General objectives and rules

The Agency will provide assistance to further develop and implement the EUROSUR framework within the scope and in line with the provisions of Regulation (EU) No 1052/2013. Improvements and adjustments to this framework are based on the Agency's change management policy which:

- provides the overarching framework for further development of EUROSUR;
- sets out the methodology to follow for launching and consulting on changes;
- allows changes to be processed in a structured way;
- sets out the types of changes;

[56] See principles b), d) and e) in the Annex to Regulation (EU) No 1052/2013.

- identifies the decision-making process and the people and organisations responsible for this;
- provides information on technical tools to be used for submitting requests and obtaining feedback;
- ensures a secure system development lifecycle and consistency with ECN security accreditation;
- ensures that the approach to change focuses on end users and their needs.

Any changes must comply with Regulation (EU) No 1052/2013 and be processed in line with EUROSUR governance structures. The Agency's Senior Business Owner for EUROSUR has decision-making powers. S/He is responsible for the entirety of the Agency's business processes and is ultimately accountable for delivery of the Agency's products and services. The Senior Business Owner is:

- advised by the EUROSUR Expert Group (EEG);
- supported by the Agency's internal coordination mechanisms;[57]
- assisted by the EUROSUR Change Advisory Board.

If any strategic decisions on the development of EUROSUR are required, the Agency's Management Board may be asked to provide its advice. The Senior Business Owner may delegate some of his/her decision-making powers to other entities within the Agency, in particular to the EUROSUR Change Advisory Board, whose chairman reports to and is supervised by the Senior Business Owner.

4.4.2 Change types

A change within the EUROSUR framework is, within the limits and requirements of Regulation (EU) No 1052/2013, to be understood as the addition, modification or removal of any component of the system, affecting its performance. The change can be initiated by an individual Member State or a group of Member States, via their NCC(s) or by the Agency.

- Major changes (changes that have a high impact on internal workflow, or involve a high number of stakeholders, high level of complexity, interruption of current workflow, or are of strategic or tactical value) must be processed using the change management structure and internal coordination mechanisms. They require approval by the Senior Business Owner.
- Minor/normal changes (changes that have a low impact on ongoing processes and product/service delivery, low level of complexity, or are of a technical nature) do not require senior management involvement and should be processed by the Change Advisory Board accordingly. They might require additional consultation, using internal coordination mechanisms.
- Non-standard changes (changes that are out of scope of the standardised procedures) must be assessed by the Change Advisory Board and processed as minor or major changes, depending on their impact and complexity. They might require additional consultation using internal coordination mechanisms.

[57] Internal coordination mechanisms of the Agency consist of internal cooperation/consultation between the Agency's units and include structures and procedures to initiate and process changes to EUROSUR as well as being responsible for implementing these on behalf of the Agency.

- Quick patches/fixes (mostly IT related) or standard changes (changes following standardised model procedures that have been communicated to all stakeholders) do not require a reaction from governance structures and are dealt with by the relevant units in the Agency.

Urgent change requests, relating to emergency issues, are processed using a separate procedure. Every change within the EUROSUR framework, except quick patches/fixes or standard changes, requires the submission of a change request in line with the requirements set by the Agency to facilitate the process.

4.4.3 Change process initiation by Member States

Member States can launch improvements to the EUROSUR framework through:

- the EUROSUR Expert Group; or
- the EUROSUR change register and the feedback system developed based on EUROSUR Technical Management Services' feedback tool.

The *EUROSUR Expert Group* acts as an advisory body to the Senior Business Owner by providing opinions and recommendations from end users. In this capacity it may:

- consider and advise on changes;
- draw up change proposals;
- evaluate changes submitted (including costs/benefit analysis).

The EUROSUR Expert Group or the Agency may decide to create specific sub-groups or task forces to prepare particular change requests.

The *EUROSUR change register and feedback system* is an internet-based technical tool to:

- register all change requests and monitor their processing;
- consult/examine the change concept before the change request is submitted;
- report problems and failures in the EUROSUR framework that require the change process to be launched;
- submit ideas to improve the EUROSUR framework;
- share and obtain news and participate in forums related to the operation of the EUROSUR framework;
- seek feedback and receive input from other end users.

The Agency monitors the EUROSUR change register and feedback system to process change requests made to the EUROSUR Change Advisory Board, using the Agency's internal coordination mechanisms, or to the EUROSUR Expert Group to obtain advice before the Agency makes a final decision.

4.4.4 The role of EUROSUR Change Advisory Board

The EUROSUR Change Advisory Board is a consultative and decision-making forum managed by the Agency, which carries out the following tasks:

- monitoring and making use of the EUROSUR change register and feedback system;
- collecting and logging all business or technical change requests from internal and external stakeholders, keeping track of change request process;

- assessing, prioritising and validating each change request;
- adjusting the status of the change request if necessary (e.g. from minor to standard);
- making decisions on and proposing timelines for implementing changes;
- bringing requests requiring additional advice or permission to the relevant management structures, including internal coordination mechanisms set up for this purpose;
- submitting major change requests to the Senior Business Owner for a final decision and consulting on other change requests if required;
- escalating issues to the EUROSUR Expert Group if its advice is needed;
- carrying out further consultation within the Agency if needed as a result of the proposed change's impact or complexity;
- communicating decisions and preparing an explanation if a change request is denied.

4.4.5 Rules applied to change requests

Change requests may be accepted or refused for technical, financial, legal or operational reasons. They may be also returned to the initiator asking for further reasons for the change, or the provision of additional information, including use cases, costs and impact analysis, before a final decision is made. If the change request is refused, the Agency provides the initiator with an explanation for the refusal.

The NCC is the Agency's single point of contact for processing change requests. If the proposed change has been drawn up by the EUROSUR Expert Group, it is monitored through the EUROSUR change register and feedback system. NCC findings may also trigger the initiation of a change request on behalf of Member States.

4.5 Business continuity management[58]

ISO standard 22301:2012 defines business continuity as the capability of an organisation to continue delivering products or services at acceptable predefined levels following a disruptive incident. This standard defines business continuity management as a holistic management process that:

- identifies potential threats to an organisation and the impacts on business operations that those threats, if realised, might cause; and
- provides a framework for building organisational resilience, capable of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

As the ECN is a distributed system with a node in each Member State and the Agency, continuity of service must be ensured both at national and European level.

Risks and issues threatening the smooth running of the different components of the EUROSUR framework must be identified and assessed, and NCCs and the Agency must be prepared to react appropriately if these risks materialise. NCCs and the Agency must prevent or at least minimise the potential impact of a threat or a risk which endangers the flow of information in the ECN and has an impact on the creation, maintenance and distribution of the NSP, ESP and the CPIP.

[58] See Annex to Regulation (EU) No 1052/2013.

– The Agency is responsible for examining the risks and threats to which the ECN as a whole could be exposed and ensures its stability and good functioning.

– NCCs are responsible for ensuring the efficient use of their EUROSUR node, entering their data in the ECN, and supplying the facilities required to enable their ECN node to function properly and ensure the necessary security measures have been implemented to protect the ECN node. NCCs must guarantee connectivity to NCC networks and their national systems to enable data to be used and transferred around the ECN.

These obligations must be met through developing business continuity plans within the Agency and each NCC, as described in the Memorandum of Understanding and based on the following five key steps:

4.5.1 Impact analysis

The purpose of this step is to identify the key processes and functions within the system and the impact if they become unavailable for operations.

The analysis covers functions and services provided by the Agency, the ECN and by the NCCs, categorising them as:

– *Critical functions* — cannot be interrupted for more than one hour. Unavailability of these functions needs to be addressed immediately, as they have a high impact on the functioning of the entire EUROSUR framework.
– *Essential functions* — an interruption of maximum one day is tolerable. However, these should be restored as soon as possible and, ideally, be unavailable for no longer than a couple of hours.
– *Necessary functions* — functions that are important for the proper functioning of the EUROSUR framework and crucial for NCC performance in the longer term. These can be interrupted for up to a week without affecting key deliverables; however they should be restored as soon as possible.

A business risk analysis for the ECN has been carried out as part of the accreditation process.

4.5.2 Risk management

The purpose of this step is to identify, analyse, control and monitor risks. Risks must be assessed with regard to the likelihood they might materialise and the consequences if they materialise. Typical risks include:

– loss of key assets (head office, equipment or infrastructure);
– loss of key staff (including their unavailability);

– loss of subsidiary external services (e.g. external contractual providers, loss of electricity, water and other utilities).

4.5.3 Development of a business continuity strategy and plan

The purpose of a business continuity strategy is to define the criteria for risk acceptance and the measures to mitigate unacceptable risks. All critical, essential and necessary functions must have an identified recovery time. The business continuity plan describes the procedures that guide organisations to respond, recover, resume, and restore functioning to a predefined level of operation following disruption. These plans typically include details relating to:

– the plan’s purpose, scope and users
– reference documents
– assumptions

– roles and responsibilities
– key contacts
– plan activation and deactivation
– communication
– incident response
– order of recovery for activities
– recovery plans for activities
– disaster recovery plan
– required resources
– restoring and resuming activities

These plans should be integrated in the overall business continuity plan for Member States and the Agency.

4.5.4 Communication in case of disruption

If the ECN's business continuity is disrupted, the NCC and the Agency notify each other of the incident and the possible impact, using the communication channels set out in the Memorandum of Understanding. The notification should include a description of the disruption, its impact on the ECN and whether the NCC or Agency has activated its business continuity plan. If the disruption may have a broader impact, all Member States must also be informed about the incident and its potential impact.

If a Member State or the Agency carry out tests that might have a potential impact on the overall functioning of the ECN, they inform each other in advance of the tests and their estimated effects and duration.

4.5.5 Maintenance of business continuity management

These processes and plans must be regularly maintained, adjusted and improved, to ensure that they are suitable for the current situation. This includes regular testing and exercising, taking corrective actions, and amending and auditing the processes and plans.

4.6 Communication

4.6.1 General objectives

To achieve EUROSUR's objectives, effective communication covers the following areas:

– information exchange on EUROSUR content (NSP, ESP and CPIP);
– communication between NCCs and with the Agency, as part of day-to-day work (contacts between operators etc.);
– addressing any technical or business issues (such as bugs, IT incidents, access requests, etc.), including in cases where business continuity is at stake (see Chapter 4.5).

Effective communication means that the information provided through EUROSUR is of clearer and better quality and so supports an improved reaction capability.

4.6.2 Day-to-day communication

Day-to-day communication takes place:

– at European level — between the NCCs and with the Agency;

– at national level — effective communication channels must be established between all authorities with responsibility for border surveillance, including in authorities within the chain of command for effective decision-making and providing reaction capabilities;

– inside the Agency — among the various units involved in creating the ESP/CPIP.

Day-to-day communication may take place via:

– the ECN and dedicated applications, including the EUROSUR application and videoconferencing facilities;

– telephone and email, using the contact lists (see Chapters 3.1.15 and 4.6.4);

– other platforms (e.g. Frontex One Stop Shop document repository, etc.)

Each Member State is available 24/7 via its NCC.

4.6.3 The Agency's central point of contact

The Agency has a central point of contact located in the unit responsible for current information exchange and maintaining situational awareness. This unit is the central reference point coordinating, at Agency level, all incoming and outgoing operational information in a timely and reliable manner.

This unit provides a holistic approach for NCCs and internal Agency units by monitoring and processing incoming and outgoing operational information to maintain the ESP/CPIP and increase the reaction capabilities in Member States, e.g. by coordinating the delivery of services relating to the common application of surveillance tools and facilitating communication on rapid operational responses, when needed.

As the operational gateway to the Agency, through operational communication and information management, this point of contact provides capability for:

- situation monitoring;
- situation awareness and support;
- service delivery of EUROSUR Fusion Services;
- coordination and facilitation of joint operational activities, acting as the operational link between the responsible project team at Agency level and participating actors in the field;
- emergency and crisis management;
- liaison with NCCs;
- liaison with internal Agency units.

4.6.4 Contact list

The Agency is responsible for maintaining the contact list for NCCs, which includes:

- the NCC's place in Member State structures (name of authority, etc.);
- the name and title/rank of the Head of the NCC;
- the NCC's address and service hours (office hours/duty hours);
- the NCC's email address — monitored 24/7;
- telephone number(s) for the NCC — monitored 24/7;
- the list of authorities represented in the NCC and service hours for each authority.

The NCCs must inform the Agency, without delay, of any changes to these details.

The contact details list includes the Agency's contacts for:

- operational/information exchange matters;
- service requests relating to the common use of surveillance tools;
- access management;
- technical helpdesk.

4.6.5 Communication related to day-to-day operational matters

The NCC which first receives information within EUROSUR's scope is responsible for entering it into the EUROSUR application and sharing it with relevant partners without delay.

Close-to-real time (immediate) reporting has to be provided from the field to the NCC. Reporting at national level should take place using predefined templates, so that there is a unified approach to reporting. Plans should be made in advance to ensure immediate reporting in emergencies. In emergencies, NCCs may notify other NCCs/the Agency of the ongoing situation via other means of contact such as telephone, videoconferencing, etc., using the contact details provided in the contact list.

Best practice: In monthly video-conferences between the Heads of the NCCs and the Agency operational issues are discussed.

4.6.6 Official meetings

Heads of the NCCs, representatives from relevant national authorities and the Agency meet regularly within a user-driven *EUROSUR Expert Group*.

The EUROSUR expert group, involving internal and external stakeholders, ensures exchange of experiences gained at practical level and improves coordination between internal and external stakeholders. The group's purpose is also to ensure exchanges on practical issues related to the EUROSUR framework. The group prepares and advises on technical and business issues related to the EUROSUR framework.

Technical and business oriented sub-groups may be created to support the EUROSUR expert group on an ad hoc or temporary basis.

Examples: analysis layer user group, ECN accreditation expert group, etc.

4.6.7 EUROSUR and public relations

The information included in EUROSUR should be subject to the highest possible transparency measures. However, in order not to jeopardise the outcome of ongoing operational activities/investigations, discretion must be applied as to what information is released to the public. This should be considered on a case-by-case basis by the relevant authorities.

Only the authorities who upload information to EUROSUR are authorised to discuss the details of specific incidents with the press.

If the Agency is involved in operational activities, it retains its right to use information on the outcome of these activities.

Interviews about EUROSUR should be given by the personnel dealing with and knowledgeable about the matter.

4.6.8 Language of communication

The working language of communication in EUROSUR is English. Member States ensure that all communication provided at national level is appropriately translated and clear.

5 Interagency and external cooperation principles

5.1 Agency cooperation with other EU institutions, bodies, agencies and international organisations[59]

This chapter provides guidelines for efficient information exchange and cooperation between the Agency and other EU institutions, bodies, offices, agencies and international organisations. The details of how this should be carried out are described in specific documents (e.g. working arrangements).

5.1.1 Partner organisations

The Agency coordinates and exchanges information, using secure communication lines where possible and necessary, with EU institutions, bodies, offices, agencies and international organisations, in order to make best use of the available information, capabilities and systems. The relevant stakeholders are grouped into:

- EU institutions, bodies, offices and agencies ('EU partner organisations'); and
- international organisations and bodies ('non-EU partner organisations').

When working with these partner organisations, the Agency must ensure that their mandate, legal framework and autonomy are fully respected.

5.1.2 Scope

The Agency exchanges information with EU and non-EU partner organisations for the following purposes:

1) Provision of relevant data on illegal immigration and cross-border crime to be included in the ESP/CPIP. Europol is the main partner in this area. The Agency may also work with other partner organisations, such as Interpol, MAOC-N, Commission services, eu-LISA, Eurojust, EEAS and others. The information collected in the ESP/CPIP is shared with partner organisations on a need-to-know basis and to the extent required to carry out their own mandate. Data to support and maintain the ESP/CPIP provided by Commission services, the EEAS, the FRA, the EASO (e.g. on managing migration flows, or country of origin information) and from non-EU partner organisations will be processed and combined with information from other sources, validated and then made available to Member States' NCCs by the Agency via the ESP/CPIP. If the Agency receives relevant information from two or more partner organisations, it merges this information and validates it before publishing it in the ESP/CPIP.
2) Contributions to the *common application of surveillance tools* are provided by EMSA, EFCA, SATCEN and other relevant partner organisations, as described in Chapter 3.2.8. For the acquisition of satellite imagery and the use of satellite-derived data in day-to-day operations, the Agency makes best use of the Copernicus programme.[60]

5.1.3 Legal framework

The cooperation of the Agency with third parties as referred to in Article 18 of Regulation (EU) No 1052/2013 is laid down in working arrangements and other relevant regulatory documents (e.g. service level agreements, Memorandum of Understanding) signed between the Agency and EU/non-EU partner organisations, in accordance with Article 13 of Council

[59] Article 18 of Regulation (EU) No 1052/2013.
[60] Copernicus, previously known as GMES (Global Monitoring for Environment and Security), is the European Programme for the establishment of a European capacity for Earth Observation.

Regulation (EC) No 2007/2004. This may include relevant existing cooperation instruments, or new ones if required. The rules of procedure used for information exchange will be set out in the working arrangements.

5.1.4 Communication channels

The Agency is the single point of contact for the exchange of information and cooperation with partner organisations. Since access to the ESP/CPIP is limited to the Agency and the NCCs, the Agency establishes dedicated communication channels with partner organisations.

Each partner organisation identifies the required communication infrastructure and a point of contact. Contact details (official and functional email address, mobile number and official address) for this point of contact are to be communicated to the Agency.

If the structure of the partner organisation requires more than one point of contact to be nominated, contact details and the split in responsibilities for these contact points must be communicated to the Agency.

The Agency creates and maintains a contact list for partner organisations with which it cooperates in EUROSUR.

5.1.5 Evaluation

The Agency and partner organisations analyse, develop and evaluate the outputs produced by working together in the framework of EUROSUR, with a view to identifying needs and gaps and proposing measures for improvement. These findings may trigger the Agency to initiate change process in line with the rules laid down in Chapter 4.4. The evaluation is carried out in accordance with the bilateral cooperation framework and whenever required by the operational situation. The cooperation between the Agency and partner organisations may be adapted in line with this evaluation and operational needs.

5.2 Cooperation of Member States with neighbouring third countries[61]

A well-structured and permanent exchange of information and cooperation by Member States with neighbouring third countries is key to preventing illegal immigration and cross-border crime and for contributing to the saving of migrants' lives. In order to be sustainable, this cooperation has to be reciprocal, based on mutual trust and beneficial both for the Member State(s) and third countries. It is essential that any such cooperation is carried out in full compliance with legislation on fundamental rights.

Member States can work with neighbouring third countries at international, multilateral and bilateral level.

5.2.1 International cooperation

Depending on the level of cooperation, international cooperation may include:

1) Exchange of information with and assistance from the Agency, in close coordination with the European External Action Service, Europol, Eurojust, Interpol and other relevant bodies.
2) The participation of third-country experts in programmes, projects, conferences, seminars and working groups set up by the Agency, the European Commission, Interpol, the United Nations and international organisations.

[61] Article 20 of Regulation (EU) No 1052/2013.

3) The deployment of liaison officers in EU Delegations[62] and in Member States' embassies and consulates.

4) Joint risk analysis and investigation activities with authorities in third countries.

5) Training for third-country authorities in border control activities, search and rescue, fundamental rights, etc.

6) Strengthening third countries' capacities through programmes co-financed by EU and international funds.

5.2.2 Multilateral and bilateral cooperation

Depending on the level of cooperation, multilateral and bilateral cooperation may include:

1) Liaison officer networks.

2) Regional networks, used for exchanging information via secure communication channels, exchanging liaison officers, training, strengthening surveillance capabilities and setting up coordination centres in third countries. If several Member States participate in a regional network, they must inform the Agency which of their NCCs is responsible for the exchange of information between the regional network and EUROSUR.

3) Joint operational activities (land, sea and air), including joint patrolling.

4) Training for third-country authorities in border control, search and rescue, fundamental rights, etc.

5) Strengthening capacities through donating assets and technical assistance to improve the border control capabilities of third countries.

Examples of regional networks are the Baltic Sea region border control cooperation (BSRBCC) network and the Seahorse Atlantic network.

5.2.3 Agreements

The cooperation described above takes place based on agreements and working arrangements or through regional networks established on the basis of those agreements. Before concluding any such agreement or working arrangement, the relevant Member State must notify the European Commission of the text or the relevant provisions. The Commission will verify that these provisions comply with the provisions of Article 20 of Regulation (EU) No 1052/2013. Member States must also notify the Commission of the texts of concluded agreements, and the Commission will provide the European Parliament, the European Council and the Agency with a general overview and assessment of those agreements.

Member States inform the Agency about current cooperation at operational level with third countries, as required by Article 2(2) of Regulation (EC) No 2007/2004. When concluding bilateral agreements with third countries, Member States may include provisions concerning the role and responsibilities of the Agency, after consulting the Agency about this.

If information to be exchanged with authorities in a third country belongs to an Member State or the Agency that is not part of the cooperation agreement or regional network, the NCC of the Member State wishing to share the information must send a written request to the information owner (Member State or the Agency), indicating the third country with whom the information will be shared and explaining the reasons for sharing such information. The

[62] In line with the "Concept paper on the deployment of European Migration Liaison Officers" (Council document13435/4.11.2015 JAI 790 ASIM 130 RLEX 853).

information owner (Member State or the Agency) replies to the request in writing as soon as possible. Any refusal to share information must be explained. Tacit approval is not permitted – the information owner must respond positively or negatively.

6 Monitoring and evaluation[63]

The following measures are to be taken to monitor EUROSUR's *technical functioning*:

- In its report due on 1 December 2015 and every two years thereafter, the Agency provide an overview of the implementation of the ECN, the ESP (including border sections and the allocation of impact levels) and the CPIP, and the common application of surveillance tools, describing the progress made and identifying any measures which still need to be taken to fully comply with the provisions of Regulation (EU) No 1052/2013.

- By 31 January 2016 and by the same date in each year from then on, each Member State provides an annual report on the set-up and running of its NCC and its NSP, describing the progress made during the previous year and identifying any measures which still need to be taken to fully comply with the provisions of Regulation (EU) No 1052/2013. The Commission will provide a summary in its overall evaluation of EUROSUR, due on 1 December 2016 and every four years thereafter.

The following measures are to be taken to monitor EUROSUR's *operational functioning*:

- As of 2015, in the annual report referred to above, each Member State provides a description of the measures taken at national level (with emphasis on the NCC's role) relating to those external border sections to which a medium or high impact level has been allocated.

- In its report due on 1 December 2015 and every two years thereafter, the Agency provides an overview of measures taken by Member States and by the Agency relating to those external border sections to which a medium or high impact level has been allocated. In this report, the Agency will work with the relevant Member State(s) to analyse and evaluate the measures taken at national and European level.

- In its overall evaluation due on 1 December 2016 and every four years thereafter, the Commission will assess how the EUROSUR Regulation has been applied in Member States and by the Agency.

The following measures are to be taken to monitor how fundamental rights, including the principle of non-refoulement, have been respected in the framework of EUROSUR:

- In compliance with Article 3(1) of Regulation (EC) No 2007/2004 and annexed to the Agency's report due on 1 December 2015 and every two years thereafter, the Agency's Fundamental Rights Officer may provide observations on the Agency's compliance with legislation on fundamental rights. The Consultative Forum may make recommendations to the Agency on compliance with fundamental rights when implementing the EUROSUR Regulation. To do this, the Fundamental Rights Officer and the Consultative Forum, within their given mandates, have access to all information relating to the respect for fundamental rights for all the Agency's activities within the framework of EUROSUR.

- In its overall evaluation due on 1 December 2016 and every four years thereafter, the Commission provides an assessment of the Agency and Member States' compliance with

[63] Article 22 of Regulation (EU) No 1052/2013.

legislation on fundamental rights (including personal data protection and the non-refoulement principle) when implementing the EUROSUR Regulation.[64]

- In its overall evaluation due on 1 December 2016 and every four years thereafter, the Commission provides an overview of the agreements concluded between Member States and third countries for the purposes of the EUROSUR Regulation and an assessment of whether these agreements comply with the provisions of Article 20 of Regulation (EU) No 1052/2013.

7 Handbook review and closing remarks

The Commission may amend this handbook on the basis of contributions received from the Agency and the Member States.

The Agency and the Member States may, after consultation of the European Commission, agree on and classify internal documents (catalogues, terms of reference, etc) to further specify operational, technical or any other requirements required for the implementation and day-to-day use of EUROSUR. The Commission verifies that these documents comply with the provisions of Regulation (EU) No 1052/2013 and this handbook.

[64] The Commission may use the Fundamental Rights Agency when preparing its assessment.

8 List of instruments

- Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR)
- Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
- Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
- Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)
- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- Charter of Fundamental Rights of the European Union
- Convention for the Protection of Human Rights and Fundamental Freedoms
- Convention on the Status of Refugees (1951) and its Protocol (1967)
- 1979 International Convention on Maritime Search and Rescue and other International Conventions falling under the auspices of the International Maritime Organisation

9 List of abbreviations

Agency	European Agency for Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex)
AIS	Automatic Identification System
BSRBCC	Baltic Sea Region Border Control Cooperation
CIRAM	Common Integrated Risk Analysis Model
CPIP	Common Pre-frontier Intelligence Picture
EASO	European Asylum Support Office
EBGT	European Border Guard Teams
ECN	EUROSUR Communication Network
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EEG	EUROSUR Expert Group
EFCA	European Fisheries Control Agency
EMSA	European Maritime Safety Agency
EO	Earth Observation
EPN	European Patrols Network
ESP	European Situational Picture
ETMS	EUROSUR Technical Management Services
EU	European Union
EUCI	EU classified information
EUROJUST	European Union's Judicial Cooperation Unit
EUROPOL	European Police Office
EUROSUR	European Border Surveillance System
FRA	Fundamental Rights Agency
ICC	International Coordination Centre
INTERPOL	International Criminal Police Organisation
ISO	International Organisation for Standardisation
ICT	Information and Communication Technology
JORA	Joint Operations Reporting Application
LCC	Local Coordination Centre
LRIT	Long-Range Identification and Tracking System
MAOC-N	Maritime Analysis and Operations Centre — Narcotics
MRCC	Maritime Rescue Coordination Centre
NCC	National Coordination Centre
NFPOC	National Frontex Point of Contact
NSP	National Situational Picture
RCC	Regional Coordination Centre
SATCEN	European Union Satellite Centre
SAR	Search and Rescue
SIRENE	Supplementary Information Request at the National Entry
TETRA	Trans-European Trunked Radio
UN	United Nations
VHF	Very High Frequency
VMS	Vessel Monitoring System
VPN	Virtual Private Network