Template of a programme for the AMIF, the ISF and the BMVI – Article 16(3)

CCI number	
Title in English	Programme for the Internal Security Fund
Title in the national language	Sisejulgeolekufondi rakenduskava 2021-2027
Version	1.1
First Year	2021
Last Year	2027
Eligible from	01.01.2021
Eligible until	31.12.2029
Commission Decision Number	
Commission Decision Date	
Member State amending decision number	
Member State amending decision entry into force date	

1. Programme strategy: main challenges and policy responses

In Estonia, there has been a significant change in the national strategic planning process compared to the programming of the 2014-2020 period. All strategic planning of the national needs and their financing is central; there is no separate process for programming the EU funds. The planning is source-neutral; the mapping of important strategic goals is done without determining the source of budget. The funding is decided on a rolling basis during the yearly budgeting exercises. This fundamental change in process has also affected the compilation and structure of this programme.

The ISF programme is designed to address the most pressing challenges identified at the national level and complement the national funding. Synergies and consistencies with other programmes and instruments are sought, where possible. Security is addressed in several Union programmes, coherence is integral with other EU funds e.g. AMIF and BMVI which all support actions contributing to the EU's overall security. Furthermore, synergies between the Justice programme and the Citizens, Equality,

Rights and Values Programme are relevant in terms of assisting and protecting the victims of crime and judicial training to a lesser extent but also inter-agency cooperation between relevant law enforcement authorities and ensuring connection of LEAs security-related IT-systems to ECRIS-TCN. Also, there is synergy with the EU Customs Programme 2021-27 in terms of responding to security threats and cross-border crime. Similarly, coherence with Cohesion Policy Funds, Horizon Europe and the Digital Europe programme are kept in mind in relevant areas. Simultaneously with the programming of the ISF, the planning of the use of Cohesion Policy Funds is carried out in Estonia, thereby the complementarity and prevention of any overlaps on national level is ensured. The actions to be financed will depend on the resources available and priorities at the time. The precise actions and the source of financing will be agreed during the implementation of the programme in accordance with national procedures.
Synergies with other funds (e.g. AMIF, BMVI) and agencies' toolbox will be sought and overlapping avoided by the thorough communication between the ministries, the European Commission, agencies and other relevant stakeholders.

The-long term umbrella strategy Estonia 2035 provides a coherent guidance for policy-makers in different areas. The main national strategy covering the internal security goals is the Internal Security Development Plan (ISDP). The ISDP has been developed in close partnership with all relevant partners and stakeholders (please see Section 4 for more comprehensive overview concerning their input). The priorities highlighted in the ISDP are creating secure living environment (incl. less violence); ensured internal security (incl. fight against organised crime, readiness for crisis); fast and professional help; citizenship, migration and identity administration policy that ensures Estonian development; smart and innovative internal security.

The ISDP 2020-2030 takes into account the relevant EU policies and goals. In Estonia, the responsibility for implementing various relevant policies is intertwined between several ministries and areas of government. Complementarity is sought with national strategies: e.g. Digital Agenda 2020, the general principles of Criminal Policy until 2030, National Security Concept of the Republic of Estonia, the internal security strand in the National Defence Development Plan 2017-2026 and National Radiation Safety Development Plan 2018–2027.

The main keywords that describe the challenges in Estonia cover most of the ISF objectives: cybercrime, money laundering and terrorist financing, terrorism and radicalization, serious and organised crimes, drug trafficking, financial investigations, corruption, detection and confiscating of criminal assets, trafficking in human beings, (sexual) abuse and exploitation of children, forensic capacity, crisis prevention, emergency preparedness, resilience during crisis, repulsion of cyber-attacks, chemical, biological, radiological and nuclear (CBRN) materials and explosives.

The measures to address these challenges include developments and continuity of **information and communication technologies**, smart and innovative **technological tools**, increased **analytical capacity**, (operational) **cooperation** within and between different parties and authorities as well as improved national capabilities incl. through **training** and purchase of relevant **equipment**. **Staffing** the relevant units with sufficient

number of skilled professionals is also a necessity. Other keywords are **prevention**, **early warning** and **awareness raising**. **Security research** plays an important role in developing innovative methods or deploying new technologies.

The goals of the ISF programme can be achieved with the contribution from various authorities in their area of responsibility. The involvement of civil society, other relevant partners and cooperation with the private sector is similarly essential in this area - projects of this nature as well as cooperation with third countries will also be considered when implementing the ISF programme. The support will be given as grants.

As some of the challenges remain the same, the ISF 2021-27 programme will partly focus on similar activities as those of ISFP in the period of 2014-2020.

ISF-Police 2014-2020 has provided valuable complementary resources for implementing the relevant EU *acquis*. The current programme continues to ensure coherence with the application of the Union acquis, and where appropriate, action plans, throughout the cycle of the programme and taking into account the new emerging threats. A brief overview of the state of play in **implementing the EU *acquis*** is as follows.

Estonia has been following the aims and actions of the **EU Drugs Strategy** 2013-2020 and the EU Action Plan on Drugs 2017-2020 by implementing the national strategy document The White Paper on Drug Prevention Policy, adopted in January 2014. Its main objective is to reduce drug use and the resulting harms. It follows the EU's balanced approach to drug policy and is structured around seven pillars: (i) supply reduction; (ii) universal primary prevention; (iii) early detection and intervention; (iv) harm reduction; (v) treatment and rehabilitation; (vi) resocialisation; and (vii) monitoring. The implementation and funding of drug policy activities is done through national strategies that follow the aims of White Paper and therefore the EU Drugs Strategy.

In terms of **EU information systems**, the required works stemming from the regulations are ongoing on a national level.

The **PNR** database is being developed from the ISF 2014-2020. The PNR directive was transposed in February 2019. The PIU unit was set up in May 2018 and from 15 August 2019 there is an automatic comparison of passenger data with the SIS.
According to the PNR directive Annex I, list of the PNR data also consider API data as a part of the PNR. The program will ensure the processing of API data as a part of the PNR keeping the implementation updated with the future revision of the API directive.

The **SIS** in the field of police cooperation has been developed under the ISF-Police. Interpol inquiries have been integrated into SIERNE. The recommendations of Schengen Evaluation 2018 report were considered and kept on focus when planning for 2021 and forward.

In 2018, a total of 14 Schengen Evaluation recommendations were made to Estonia in the field of police-cooperation. 5 recommendations have been fulfilled by the time of drafting this programme and others are ongoing. In May 2021 the follow-up plan for implementing the recommendations was submitted to the European Commission. One of the recommendations is planned to be financed from the ISF (see the description in SO2). Regarding the future needs stemming the future Schengen and Scheval evaluations in the field of SIS/SIRENE and Police Cooperation, they will be mostly financed from the national budget, however ISF funding could be used where appropriate.

The **PRÜM** process scheme is followed at national level, as PRÜM is an important tool for our law enforcement experts. At the very moment, development work is underway in the European Union to improve the functionality of PRÜM. There are discussions about the ways to improve the quality and speed of data exchange for example by having a central, EU level router, as well as what further data categories could be included in PRÜM. Changing more information on vehicles; additional biometrics, such as facial images are all being considered when reforming the existing framework.

Estonia participates actively in **CEPOL cooperation**. CEPOL National Unit is located in Police and Border Guard College of Estonian Academy of Security Sciences (EASS). EASS is also the Framework Partner of CEPOL. In Estonia cooperation with CEPOL is organised in the format of national network consisting of 11 agencies having responsibilities in the field of law enforcement.

The training activities for law enforcement officials will take into account the outcomes of the EU Strategic Training Needs Assessment 2022-2025 prepared by CEPOL, special attention will be given to the core capability gaps.

The principles of the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European **critical infrastructures** and the assessment of the need to improve their protection have been taken over by the Emergency Act.

There are no problems with the transposition and implementation of EU *acquis* in Estonia regarding **anti-corruption measures**. The Ministry of Justice is preparing the transposition of the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law. There is no separate EU action plan on anti-corruption and until April 2021 when EU Strategy to tackle Organised Crime 2021-2025 was adopted. It can be concluded that activities of Estonia in the area are not in contradiction to EU strategic objectives.
The Commission's 2021 Rule of Law report points out that the Estonian criminal justice system has proven its effectiveness in identifying high-level corruption cases. Measures to strengthen the preventive side include guidelines for lobbying and conflict of interests. The legislative procedure to adopt comprehensive rules on whistleblowers protection is currently ongoing. The asset declaration system was updated to oblige ministers' political advisers to submit a declaration of financial interests.

The transposition of the EU *acquis* related to **trafficking in human beings** into Estonian law has been carried out. Nevertheless, the implementation of measures by different authorities need to be further improved as not all the special measures related to treatment of victims are implemented in everyday work of authorities (e.g. special measures related to hearings). According to Article 2 of the Directive 2011/36/EU of 5 April 2011, Member States shall take the necessary measures to ensure that the following intentional acts are punishable: the recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Estonia is dedicated to the full compliance with the definition of the Anti-trafficking Directive as a primary point of reference.

Until April 2021 the latest EU level strategic guidelines in the area of trafficking in human beings were provided in the Communication from the Commission to the European Parliament and the Council „Reporting on the follow-up to the EU Strategy towards the Eradication of trafficking in human beings and identifying further concrete actions". Estonia is taking relevant actions to address the three priorities outlined in the communication and contributes in relation to the priorities set in the new EU Strategy on Combatting Trafficking in Human Beings.

Estonia has transposed Directive 2017/853/EC defining a set of common minimum rules for the control of the acquisition and possession of **firearms** in the EU, as well as the transfer of firearms to another EU country into national law. The 2017 revision brings substantial improvements to security by making it harder to acquire legally certain high capacity weapons, such as automatic firearms transformed into semi-automatics. The firearms directive also strengthens cooperation between EU countries by improving the exchange of information between EU countries (Estonia has been using IMI since September 2019), and brings substantial improvements to traceability of firearms by improving the tracking of legally held firearms, to reduce the risk of diversion into illegal markets. Commission Implementing Directives (EU) 2019/69 and (EU) 2019/68 have also been transposed into Estonian law. Estonia follows the implementing regulation on common minimum standards for deactivation of firearms. All deactivated firearms are registered by the Estonian Police and their records are stored in the register of service and civilian weapons.

The government of Estonia is in process of renewing its priorities for the **fight against terrorism** in the Internal Security Development Plan (ISDP) 2020-2030. The Strategy will cover all the necessary factors and developments regarding counter-terrorism and violent extremism. ISDP priorities are in conformity with the UN CT Global Strategy, as well as the main principles and priorities of the UN, EU, CoE, OSCE and international law (incl. the protection of human rights). The ISDP is partly restricted.

In December of 2018, the Estonian Parliament passed a bill, which implements UN resolution 2178, the CoE's Convention on the Prevention of Terrorism Additional Protocol (CETS 217) and EU Directive 2017/541 into national law. Among other things,

the bill expanded the notion of victims of terrorism and the elements of crime for the crime of terrorism. The Estonian Parliament adopted amendments to the Penal Code, the Money Laundering and Terrorism Financing Prevention Act and Victim Support Act in December 2018 in accordance with the directive of the EU. The bill also brings Estonian legislation in line with the UN resolution and additional protocol of the Council of Europe convention on the prevention of terrorism. The Chemicals Act was amended with additional requirements to oblige prior authorisation for handling hazardous chemicals and the state supervision and notification of suspicious transactions as well as of loss and theft of the explosive precursor(s). The field of security of radioactive sources is regulated by Radiation Act that is in accordance with EU Council directive 2003/122/Euratom and other international conventions and standards. Estonia is in the process of developing additional capacity to identify and interrupt terrorism-related activities on the internet (the EU initiative to counter terrorist content online in cooperation with private sector, incl. the EU Internet Forum). Web constables (police officers working on the internet) cooperate with the Internet Referral Unit of the Europol Counter Terrorism Centre (ECTC) on countering illegal web-content and the violent propaganda.

The **Anti Money Laundering Act** which transposes the Fifth AMLD directive has been adopted in July 2020.

Regarding **cybercrime**, Estonia has set up legislation and implementation of Budapest Convention and penalisation of illicit activities. Internal operative cooperation between law enforcement and judicial authorities is working well and Estonia is looking forward to new legislation regarding the e-evidence.

Estonia has ratified the Council of Europe Convention on the **Protection of Children against Sexual Exploitation and Sexual Abuse** (the Lanzarote Convention). Estonian law is in conformity with the criminal law provisions of the Lanzarote Convention. The activities required for ratification of the Convention are specified in the "Development Plan for Children and Families for 2012–2020" and in the "Violence Prevention strategy for 2015–2020". The topics are also covered in "Action Programme of the Government of the Republic for 2019–2023", which highlights combating sexual crimes related to minors and targeting perpetrators.

Unfortunately it is not feasible to overcome all the current challenges described in the next section solely with the help of the ISF funding. This programme seeks to address these to the maximum extent possible while also leaving a degree of flexibility to be able to respond to future events and changing priorities. The actions to be financed will depend on the resources available and priorities at the time. The precise actions and the source of financing will be agreed during the implementation of the programme in accordance with national procedures.

The programme design and strategy takes into account the administrative capacity and governance rules for efficiency and wherever possible simplification measures will be implemented to reduce the administrative burden and enhanced efficiency, effectiveness and economy.

2. Specific objectives

2.1. Specific objective 1 - to increase the exchange of information among and within the Union law enforcement and other competent authorities and other relevant Union bodies as well as with third countries and international organisations

2.1.1. Description of a specific objective

Creating and modernising different secure information systems and e-solutions is a key when ensuring high level of security. As digitalisation has been one of Estonian flagships for years, it has resulted in a shortage of funding and experienced developers in the market. At the same time, new requirements for the Member States to ensure the full and uniform implementation of the Union *acquis* on security supported information exchange and in relation to Europol data must be met. Gaps in the EU information architecture must also be addressed with appropriate tools. Estonia has successfully set up and adapted national IT systems to ensure the effective connection to security relevant Union information systems and this is an on-going effort.

Estonia plans to use the ISF funding mainly for setting up, adapting and maintaining ICT systems contributing to the objectives of the Fund. It is also necessary to guarantee training of the use of the systems.

The current strategy is that the potential activities considered under this specific objective will mostly focus on the implementation measure (d) (supporting relevant national measures) from Annex II of the ISF regulation. Implementation measure (a) is also a priority - ensuring the uniform application of the Union *acquis* on security by supporting the exchange of relevant information.

If the need arises, implementing measures (b) and (c) may also be considered at later stage of implementation. There are no specific actions planned at the time of programming.

The planned addressing of the implementation measures in Annex II and examples of actions are as follows.

(a) Ensuring the uniform application of the *Union acquis* on security by supporting the exchange of relevant information for example via Prüm, EU PNR and SIS, including through the implementation of recommendations from quality control and evaluation mechanisms such as the Schengen evaluation mechanism and other quality control and evaluation mechanisms.

The current situation concerning the application of the relevant legislation (PNR, SIS, PRÜM) is described in Section 1.

One of the priorities is to keep ensuring further developments and maintenance of the **PNR**. The PNR database has been developed in the frame of the ISF 2014-2020 programme but continuous funding is essential to build on the results of this project. Several study visits are planned in addition to further developments to ensure the

reliability of the system and guarantee the compliance with the requirements of the PNR directive. PNR database interacts with the Europol Information System.

The new functionalities in **SIS** should be completed by 2022. Should there be any changes in the timeline or new agreements on SIS in the future; ISF funding may be considered for this. In addition, the proposed measures to establish the **interoperability** between EU large-scale information systems need to be continuously addressed. Estonia plans to use the BMVI programme for this purpose. However, should the need arise, developments necessary to meet the objectives of the ISF regulation may also be considered from this programme.
Funding of development projects related to Prüm will be considered where appropriate.

An indicative list of actions in connection with Annex III include:

- Setting up, adapting and maintaining ICT systems that contribute to the achievement of the ISF objectives, training on the use of such systems, improving the interoperability components and data quality of the systems;
- financing the cost of staff involved in the actions that are supported by the Fund or actions that are supported by the Fund or actions requiring involvement of staff for technical or security-related reasons.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- Projects which aim to improve the interoperability of EU information systems and national ICT systems, insofar as provided for by Union or Member State law.

(d) Supporting relevant national measures including the interconnection of security-relevant national databases and their connection to Union databases when foreseen in relevant legal bases, if relevant to implement the specific objectives set out in Article 3(2)(a).

Main focus of this programme shall be on supporting the relevant national measures. There are several challenges to better collect, analyse and share information within and between the relevant competent authorities.

It is important that all offenses are dealt with as expeditiously as possible and that the competent authorities have legitimate access to the necessary national and international databases. To this end, the relevant (national) information systems and databases and their interoperability need to be developed, taking into account information security measures and ensuring effective supervision and enforcement.

There are still areas in Estonia where data exchange is not digital and much work is done manually. The **criminal proceedings** are not fully **digitised** which hinders the speed of expertise and does not provide the maximum effective life cycle of evidence. The interaction between the police investigator and the forensic scientist concerning a specific case file still needs to be improved with the use of technology. There is a need

for new nationwide monitoring application (e.g. people, vehicles, objects), connected to the SIS and ensuring the fulfilment of international obligations in the fight against terrorism and serious and covert crimes (e.g. cybercrime, money laundering, sexual offenses against children, etc.). Estonia plans to invest both structural funds and national budget into this area; ISF funding is also considered.

There is a shortage of resources for the development of **digital forensics** in Estonia. As crimes move more to the Internet and digitalisation increases, the capacity of the relevant authorities should be increased to cope with the volume of work. There are shortcomings in ICT tools and sector-specific training, which are often funded on a one-off basis, leading to a lack of systemic and sustainable capacity. There is a need for automated solutions for the operative performance of works.

The **surveillance capacity**, incl. data gathering during surveillance activities, and relevant information exchange within and by the criminal police needs to be improved, incl. the upgrading of the national systems and purchasing relevant (ICT) equipment. The operational surveillance procedure tool used by the Estonian law enforcement authorities needs to be updated. It is necessary to develop a new surveillance module to conduct surveillance and tactical analysis as a whole in a single environment with the possibility of performing various queries (incl. to relevant EU information systems) and exchanging information. The surveillance system will be connected with the Europol Information System (EIS) and the SIS.

Money laundering, funding most of the serious and organised crime, is one of the main drivers in the field. To enhance and facilitate the accountability of corporate service providers, financial institutions and virtual currency service providers to prevent **money laundering and terrorist financing**, an appropriate portal for reporting needs to be introduced.

Estonia outsourced a development of risk assessment methodology to put together a new risk assessment for money laundering and terrorist financing in Estonia. Several working groups started in autumn 2019 and the national risk assessment was approved in April 2021.

The Internet has also become an important tool for **terrorist** groups, distributing propaganda and influencing, recruiting and mentoring terrorist henchmen. One of the priorities is to increase the capability of monitoring, detecting and removing **terrorist content online**; text and data analysis for fighting terrorism and facilitate relevant information exchange within and among Member States. The implementation of EU regulation on countering terrorist content online should be supported by EU-wide IT solutions, supporting interoperability and de-confliction of data, that could be provided by the EU (Europol). At the same, effort is needed on a national level as well – necessary technical tools and systems must be in place to contribute to this objective.

Developing capacities of relevant authorities to deal with **open source intelligence** is a priority that needs funding and different sources, incl. the ISF are considered for this purpose.

An indicative list of actions in connection with Annex III include:

- setting up, adapting and maintaining ICT systems that contribute to the achievement of the ISF objectives, training on the use of such systems, improving the interoperability components and data quality of the systems;
- financing of equipment;
- financing the cost of staff involved in the actions that are supported by the Fund or actions that are supported by the Fund or actions requiring involvement of staff for technical or security-related reasons.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- projects which aim to improve the interoperability of EU information systems and national ICT systems, insofar as provided for by Union or Member State law.

Operating support:

Estonia plans to use operating support to better contribute to the achievement of the objectives of the ISF programme. The use of operating support enables to maintain capabilities which are crucial to the Union as a whole.

It is necessary to increase the staffing of the national PIU within the Estonian Police and Border Guard Board (PBGB). The PIU analyses passenger lists, processes post-hit information 24/7 and exchanges information with their counterparts. Recruiting additional officials to the PIU is vital to ensure the required level of data exchange.

There is a consistent need to ensure the maintenance of the PNR system (e.g. security and software upgrades, infrastructure costs - costs required to maintain the servers, licenses, disk space, etc.)

In the field of digital forensics the yearly costs of special software (upgrades, fees, licences) must be guaranteed to deal with the identification, collection, handling and storage of digital evidence.

In the field of cybercrime and OSINT, the yearly maintenance costs of special software and network equipment must be covered to increase and maintain the capacity of the police to systematically manage, analyze and extract incoming information.

For all the mentioned areas, the final beneficiary is the PBGB which is by the statute responsible for security and public order in the state and the investigation and prevention of offences. Depending on national arrangements, funding related to the maintenance of ICT systems may be directed to the IT and Development Centre, Ministry of the Interior which by the statute is responsible for providing necessary ICT services to the Ministry and its area of government.

The possibility of financing other activities is not ruled out.

Financial instruments: n/a.

2.1.2 Indicators

Reference: Article 22(4)(e) CPR

Table 1: Output indicators					
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Milestone (2024)**	**Target (2029)**
SO1	*O.1.1*	*Number of participants in training activities*	*Absolute number*	*12*	*32*
SO1	*O.1.2*	*Number of expert meetings/workshops/study visits*	*Absolute number*	*2*	*7*
SO1	*O.1.3*	*Number of ICT systems set up/adapted/maintained*	*Absolute number*	*3*	*9*
SO1	*O.1.4*	*Number of equipment items purchased*	*Absolute number*	*6*	*6*

Table 2: Result indicators										
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Baseline or reference value**	**Baseline measurement unit**	**Reference year**	**Target (2029)**	***[Measurement unit for target]*[1]**	**Source of data [200]**	**Comments [200]**
SO1	*R.1.5*	*Number of ICT systems made interoperable in the Member States/ with security relevant EU and decentralized information systems/with international databases*	*number*	*0*	*numnber*	***2021***	***1***	*Abslolute numnber*	*Project reports*	
SO1	*R.1.6*	*Number of administrative units that have set up new or adapted existing information exchange mechanisms/procedures/tools/guidance for exchange of information with other Member States/EU agencies/ International organisations/ third countries*	*numnber*	*0*	*numnber*	***2021***	***1***	*Abslolute numnber*	*Project reports*	
SO1	*R.1.7*	*Number of participants who consider the training useful for their work.*	*share*	*0*	*share*	***2021***	***22***	*Abslolute numnber*	*Project reports, participant feedback survey*	
SO1	*R.1.8*	*Number of participants who report three months after the training activity that they are using the skills and competences acquired during the training*	*share*	*0*	*share*	***2021***	***22***	*Abslolute numnber*	*Project reports, participant feedback survey*	

2.1.3 Indicative breakdown of the programme resources (EU) by type of intervention

Reference: Article 22(5) CPR and Article 13(18) of the BMVI Regulation or Article 13(12) ISF Regulation or Article 16(12) AMIF Regulation

[1] *The Council's partial mandate added this column.*

Table 3			
Specific objective	**Type of intervention**	**Code**	**Indicative amount (Euro) EU contribution**
SO1	IT-systems, interoperability, data quality, communication systems (excluding equipment)	001	11 159 912.66
	Training	005	120 000
	Exchange of best practices, workshops, conferences, events, awareness raising campaigns, communication activities	006	39 893
	Equipment	008	804 750

2.2 Specific objective 2 - to intensify cross-border joint operations among and within the Union law enforcement and other competent authorities in relation to serious and organised crime with a cross-border dimension

2.2.1 Description of a specific objective

Estonia is active both in bilateral and multilateral cross-border (operational) cooperation at Union level to combat the important serious and organised crime threats to the EU.

There is tight cooperation in operational matters between the Estonian Criminal Police and their counterparts in neighbouring countries in the area of **drug trafficking**. Several Joint Investigation teams have been formed. In addition to competent authorities within and Between Member States, cooperation with international organisations (Europol, Interpol, CEPOL, EMCDDA, UNODC, DEA, etc.) needs to be enhanced. Both the Estonian police and customs authority have placed their Liaison Officers at Europol to facilitate day-to-day information exchange. Trainings, exercises, mutual learning and specialised exchange programmes are useful tools for this purpose. Focus must be on the current trends – notably technological developments and the spread of synthetic opioids, incl. fentanyls. It is crucial to respond better to a globalised drug market by strengthening partnerships between Member States' authorities and other relevant partners, incl. third countries, where relevant.

In the **fight against terrorism**, the Estonian law enforcement agencies are supported by international cooperation within the EU, the Counter Terrorism Group CTG, and the European Counter Terrorism Centre at Europol, information exchange at Interpol, counter-terrorism cooperation with UN, NATO, Council of Europe, OSCE and bilateral relations with partner countries.

Coordination and cooperation of law enforcement authorities and other competent authorities dealing with **organised crime** is vital. In the framework of the EU Policy Cycle for organised and serious international crime: EMPACT 2022+, Estonia is planning to Estonia participate in the operational action plans for the following areas: excise fraud, Missing Trader Intra Community (MTIC) fraud, new psychoactive substances and synthetic drugs, irregular migration, attacks against information systems (cybercrime), sexual exploitation of children (cybercrime), fraud with non-cash means of payment (cybercrime), firearms smuggling, environmental crime and organised property crime.

It is important for Estonia to emphasise the enhancement of EU inter-agency security cooperation (joint activities, information sharing, etc.). Estonia itself has contributed to this when the first Europol-FRONTEX Management Board joint meeting was organised under the auspices of the Estonian Presidency of the Council of the EU and the cooperation principles and activities were agreed.

Under this specific objective Estonia plans to use the ISF funding mainly for increasing coordination and improving inter-agency cooperation of competent authorities at national and Union level and with third countries, where relevant.

The current strategy is that the potential activities of this specific objective will form the most modest part of the programme. The planned focus of this specific objective is to contribute to implementing measures (a): concerning the increased law enforcement operations between Member States, with special emphasis on operational cooperation mechanisms in the context of EMPACT (b) and (c): improving inter-agency cooperation at Union level between Member States, and the relevant Union bodies, offices and agencies as well as at national level among the national authorities; also to increase coordination and cooperation of law enforcement and other competent authorities within and between Member States.

The minimum percentage set for this SO is not reached. This decision stems from the nature and amount of cross-border (joint) operations which cannot be forecast. These operations arise on a rolling basis in each field and Estonia continues to finance these from the state budget when the need occurs or use specially earmarked funds (e.g. funding provided by the Commission). Operational cooperation is of utmost importance and Estonia has and will continue actively participate both in bilateral and multilateral cross-border (operational) cooperation as described in the beginning of this Section. Moreover, there are several actions planned under the SO3 which have a broader purpose and therefore also contribute to the objectives of the SO2 (e.g. study visits and enhancing cooperation in the field of preventing and tackling corruption, international cooperation in preventing and combating cybercrime).

The current strategy takes into account the country's actual needs and challenges. While using additionally the state budget and other relevant funding possibilities, allocating resources for this specific objective below the level stipulated in the ISF regulation does not jeopardise the achievement of the objective.

The planned addressing of the implementation measures in Annex II and examples of actions are as follows.

(a) Increasing the number of law enforcement operations involving two or more Member States, including, where appropriate, operations involving other relevant actors, in particular through facilitating and improving the use of joint investigation teams, joint patrols, hot pursuits, discreet surveillance and other operational cooperation mechanisms in the context of the EU policy cycle, with special emphasis on cross-border operations.

To reduce excise criminality and excise tax gap in the Baltic region and EU overall, the efficiency and capabilities of the relevant authorities in fight against shadow economy (illegal tobacco, fuel, alcohol) is planned to be increased with the support of ISF.

In cooperation with Spain, several EU member states and third countries (incl. Norway, UK, USA), Frontex and Europol, an European Operational Team (EOT) will be established in the Spanish region 'Costa del Sol', to develop and implement a joint investigative and operational strategy against the main criminal organisations.

An indicative list of actions in connection with Annex III include:

- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence;
- education and training for staff and experts in relevant law enforcement authorities and administrative agencies;
- financing of equipment.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- Projects which aim to fight the most important threats posed by serious and organised crime, in the framework of EU policy cycle/EMPACT operational actions.

(b) Increasing coordination and cooperation of competent authorities within and between Member States and with other relevant actors, for example through networks of specialised national units, Union networks and cooperation structures, Union centres.

Pursuant to Council Implementing Decision No. 10388/19, in the framework of the Schengen evaluation of Estonian police co-operation, a recommendation has been made that Estonia should develop an interactive and user-friendly **e-learning solution on international police cooperation** based on practical situations and cases. This recommendation is planned to be addressed with the support of the ISF.

In 2019, the Estonian Social Insurance Board identified and assisted 67 victims or alleged victims of **trafficking in human beings.** This is a significant increase compared to 2018 when 12 (alleged) victims were identified. Investigative bodies and victim support organisations continuously carry out international cooperation in criminal matters and in cases with suspicion of trafficking in human beings. Cooperation is important to prevent exposure to human trafficking in host countries and to break up the organised crime groups mediating prostitutes and illegal labour force to reduce trafficking problems in Estonia. Therefore, one of the priorities for Estonia is **operational level cooperation** with third counties, establishing and maintaining reliable contacts, providing training and introducing monitoring methods developed by the Estonian Police and Border Guard Board and if necessary setting up JITs.

An indicative list of actions in connection with Annex III include:

- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence;
- education and training for staff and experts in relevant law enforcement authorities and administrative agencies.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

(c) Improving inter-agency cooperation at Union level between the Member States, and between Member States, and relevant Union bodies, offices and agencies as well as at national level among the competent authorities in each Member State.

It is essential to explore ways to improve the **cross-border police and customs cooperation** with the involvement of relevant EU bodies (e.g. Europol, EUROJUST). Criminal investigation officers from Estonian customs and police authorities need to be better prepared and informed to prevent and combat all forms of serious and international crime (e.g. drugs, trafficking in human beings, firearms trafficking, euro counterfeiting, money laundering). The secondment of officers for traineeships to the Estonian Liaison Office of Europol is a useful way to promote and improve the effectiveness of transnational operational cooperation (e.g. the use of Joint Investigation teams' capabilities, Joint Analyst Teams (JAT), Controlled Delivery (CD), and other possibilities offered by Europol, for example the Analysis Work Files and SIENA network), cooperation with Europol Counter Terrorism Centre and its units, incl. CBRN, demining and special tactics.

Estonian customs authorities would also benefit from closer operational cooperation with other EU customs administrations for better gathering and analysing information; to identify targets of organised crime; and gathering evidence in criminal proceedings. Study visits may be organised to serve this purpose.

Enhancing preparedness, early warning and response to threats and crisis requires greater cooperation between the authorities involved in CBRNe events, incl. the need to develop international cooperation under the RescEU, EU CBRNe Action Plan and threat assessments on CBRNe and terrorism. Trainings, guidelines, regulations, exercises, case studies, joint investigation teams, testings, participation in seminars and conferences on a national level and abroad contribute to this end.

It is also necessary to enhance inter-agency cooperation between first responders in the rescue services on how to safely react to calls concerning security incidents. This is an area which goes beyond the basic training of rescue services but is essential when co-responding with the police services. The knowledge and best practices of partners from other Member States is similarly crucial

An indicative list of actions in connection with Annex III include:

- actions that improve resilience as regard emerging threats, including chemical, biological, radiological and nuclear threats;
- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence;
- education and training for staff and experts in relevant law enforcement authorities and administrative agencies.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

Operating support:
The current strategy does not foresee using the operating support under this specific objective. However, when the need occurs, operating support may be considered.

Financial instruments: n/a.

2.2.2 Indicaors

Reference: Article 22(4)(e) CPR

Table 4: Output indicators					
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Milestone (2024)**	**Target (2029)**
SO2	***O.2.1***	*Number of cross-border operations*	***number***	***0***	***1***
SO2	***O.2.1.1***	*Number of joint investigation teams.*	***number***	***0***	***1***
SO2	***O.2.2***	***Number of expert meetings/workshops/study visits/common exercises***	***number***	***37***	***92***
SO2	***O.2.3***	***Number of equipment intems purchased***	***number***	***200***	***830***

Table 5: Result indicators										
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Baseline or reference value**	**Baseline measurement unit**	**Reference year**	**Target (2029)**	***[Measurement unit for target][1]***	**Source of data [200]**	**Comments [200]**
SO2	*R.2.8*	*Number of administrative units that have developed/adapted existing mechanisms/procedures/tools/guidance for*	*number*	*0*	*number*	*2021*	*18*	*number*	*Project report*	

[1] *The Council's partial mandate added this column.*

		cooperation with other Member States/EU agencies/International organisations/third countries								
SO2	*R.2.10*	*Number of Schengen Evaluation Recommendations addressed*	*number*	*0*	*number*	*2021*	*1*	*number*	*Project report*	

2.2.3 Indicative breakdown of the programme resources (EU) by type of intervention

Reference: Article 22(5) CPR and Article 13(18) of the BMVI Regulation or Article 13(12) ISF Regulation or Article 16(12) AMIF Regulation

Table 6			
Specific objective	**Type of intervention**	**Code**	**Indicative amount (Euro) EU contribution**
SO2	Joint investigation teams and other investigations	003	324 900.2
SO2	Training	005	371 250
SO2	Exchange of best practices, workshops, conferences, events, awareness raising campaigns, communication activities	006	862 500
SO2	Equipment	008	198 751

2.3 Specific objective 3 - to support effort at strengthening the capabilities in relation to combatting and preventing crime including terrorism in particular through increased cooperation between public authorities, civil society and private partners across the Member States

2.3.1 Description of a specific objective

When aiming to strengthen the capabilities of the national authorities in relation to combating and preventing crime, having motivated, skilled and informed people is the key. **Training**, **shared knowledge** and **awareness raising** are crucial in this respect. On the other hand, the need for **modern technology**, incl. **IT tools**, and **equipment** cannot be overlooked.

The focus of this specific objective is planned to be on the implementing measures (a) increasing the law enforcement training, exercises and mutual learning; and (d) acquiring relevant equipment to increase preparedness, resilience and adequate response to security threats. The potential activities will also address the implementing measures (b) and (c).

If the need arises, implementing measure (e) may also be considered at later stage of implementation.

The planned addressing of the implementation measures in Annex II and examples of actions are as follows.

(a) Increasing training, exercises and mutual learning, specialised exchange programmes and sharing of best practice in and between Member States' competent authorities, including at local level, and with third countries and other relevant actors.

There is constant need for systematic training in different areas. Training of law enforcement officers has been an important part in the 2014-2020 ISFP programme and this is also a priority in 2021-2027 period. Estonia has also benefited greatly from CEPOL trainings as different authorities have taken part in CEPOL residential activities, webinars, online-trainings, workshops and exchange programs. However, there is also a need for more specific trainings which CEPOL does not offer. Some specific trainings are planned to be financed with the ISF support. The national CEPOL unit was consulted on the design of training activities in the ISF programme to avoid overlaps. The principal rationale for including specific training actions in the programme is that CEPOL generally organizes basic or intermediate level trainings, there is less focus on more specific topics relevant for the advanced level specialists in the narrower fields. In addition, the CEPOL trainings and study visits are for limited numbers of participants per Member State and this is not always sufficient, especially for highly specialised units. In any event, all training activities will be coordinated with CEPOL.

Effective fight against **cybercrime** requires targeted action and is one of the priorities in the ISF programme. Various data thefts and data leaks, ransomware claims and online payment fraud have become commonplace problems in Estonia. Citizens, businesses and public authorities need to be aware of the dangers of ICT and be willing and able to protect themselves. Investigation of cybercrime requires very specific knowledge and skills on how to use digital evidence. The relevant law enforcement authorities need to be sufficiently staffed, trained and equipped to collect and analyse information at the necessary level and ensure the sustainability of activities. In order to alleviate these shortcomings, it is planned to finance activities under both measure (a) and measure (d) – trainings and study visits plus necessary technology and equipment.

Awareness raising on **anti-corruption** activities have become more successful over the years. Corruption offences registered in Estonia: 291 offences in 2017; 376 offences in 2018 and 72 offences in 2019. Detection of high-profile corruption cases continues to be a priority. As corruption is increasingly hidden in Estonia, there is a need for specialisation and systemic collection and analysis of information, which can lead to better detection and prosecution of such crimes. Investigating corruption and **other covert crimes**, requires the provision of tools and professional skills obtained through training, exchange of best practice with external partners, large-scale capture of electronic information and analysis of evidence. Emphasis is also on raising awareness and conducting studies in the field for better policy decisions.

An indicative list of actions in connection with Annex III include:

- education and training for staff and experts in relevant law enforcement authorities and judicial authorities and administrative agencies, taking into account operational needs and risks analyses, in co-operation with CEPOL and , when applicable, the European Judicial Training Network;
- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence;
- financing the cost of staff involved in the actions that are supported by the Fund or actions that are supported by the Fund or actions requiring involvement of staff for technical or security-related reasons.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- Projects which aim to prevent and fight cybercrime, in particular child sexual exploitation online, and crimes where the internet is the primary platform for evidence collection.

(b) Exploiting synergies by pooling resources and knowledge and sharing best practices among Member States and other relevant actors, including civil society through, for instance, the creation of joint centres of excellence, the

development of joint risk assessments, or common operational support centres for jointly conducted operations.

Not all extremism leads to violence, but it is important for society, especially parents, teachers, youth workers and officials, to set an example, and intervene to ensure security on both sides. It is important to train primary officials and professionals to recognize the first signs of **radicalisation** and to be able to assess risks and act accordingly in a sensitive way while respecting the fundamental rights of individuals. More than 2000 first level practitioners have been trained in the past under the leadership of the Estonian Ministry of the Interior and the Academy of Security Sciences. In the future, a more systematic approach to training is planned. It is necessary to continue developing the expertise of various professionals, also with the support of international networks such as RAN and ESCN, and to become familiar with practices in partner countries

To make full use of the potential of the Estonian Academy of Security Sciences (which is also the CEPOL National Unit in Estonia), it could be developed into a **center of excellence for internal security** (e.g in the domains of anti-radicalisation and counter-terrorism, fight against organised crime and cybercrimes; the use of AI). The Center would support planning and strategic development in the field through research, analysis and training, in coordination with CEPOL.

An indicative list of actions in connection with Annex III include:

- education and training for staff and experts in relevant law enforcement authorities and judicial authorities and administrative agencies, taking into account operational needs and risks analyses, in co-operation with CEPOL and , when applicable, the European Judicial Training Network;
- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- projects which aim to prevent and counter radicalisation.

(c) Promoting and developing measures, safeguards, mechanisms and best practices for the early identification, protection and support of witnesses, whistle-blowers and victims of crime and to develop partnerships between public authorities and other relevant actors to this effect.

The biggest challenge in Estonia in the **fight against trafficking in human beings** is the lack of funding of prevention activities. Prevention and awareness-raising activities and training are provided on a small scale and with small repetition interval. Joint trainings for officials dealing with trafficking in human beings are necessary to raise the competence and improve the implementation of EU *acquis*. There is a need for greater awareness of third-country nationals entering Estonia and education of young people at

school. Also the relevant training for law enforcement authorities. According to the data from the Labour Inspectorate and the Social Insurance Board, the number of labour disputes with foreigners is increasing and the number of foreigners seeking help from the anti-trafficking hotline is increasing. Educational tools have been produced for schools (supported by the ISF 2014-2020 project), but to facilitate their use, the training scope needs to be widened to include trainers going to schools to adequately change young people's attitudes and future behaviors to prevent trafficking.

Also, the competence and skills of officials, volunteers and other notifiers involved in the fight against trafficking in human beings will be increased on state and local level in order to increase the level of identification of possible victims overall in Estonia.

It is necessary to carry out information campaigns, to work closely with communication companies and education institutions to prevent the **sexual abuse of children.** The idea is to use different expertise and activities for cross-cutting prevention. The purpose is to explore how prevention opportunities can include different parties in new and innovating ways. There is also a need to raise the awareness (with appropriate long-lasting material and campaigns being worked out) and skills (special trainings in Europe and in Estonia) of adults who come into contact with young people to spot victims of abuse and to provide appropriate assistance (such as police officers, child protection officers, teachers, doctors as well as parents). We will offer special trainings to child hotline workers to give appropriate counselling in case of child sexual abuse cases online. The trainings will take into account the Council Conclusions on combatting the sexual abuse of children (12862/19). Raising the capability to identify victims would lead to better safeguarding of children and apprehend offenders in early stages of the activities. The third line of activities is to carry out research and evaluation of programs/services preventing the sexual abuse of children in Estonia.

An indicative list of actions in connection with Annex III include:

- Actions that improve resilience as regards emerging threats, including trafficking via online channels;
- education and training for staff and experts in relevant law enforcement authorities and judicial authorities and administrative agencies, taking into account operational needs and risks analyses, in co-operation with CEPOL and , when applicable, the European Judicial Training Network;
- providing support to thematic or cross-border networks of specialised national units and national contact points to improve mutual confidence, the exchange and dissemination of know-how, information, experience and best practices, the pooling of resources and expertise in joint centres of excellence.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the actual needs and available resources.

An indicative list of actions in connection with Annex IV include:

- Projects which aim to prevent and fight cybercrime, in particular child sexual exploitation online, and crimes where the internet is the primary platform for evidence collection.

(d) Acquiring relevant equipment and setting up or upgrading specialised training facilities and other essential security relevant infrastructure to increase

preparedness, resilience, public awareness and adequate response to security threats.

Preparedness for **CBRNe** and **HAZMAT** incidents need more attention, given the changed nature of threats in Europe. It is estimated that over half a million World War II explosives are still in the Estonian soil - the accessibility of these explosive substances is an essential internal security problem in Estonia and carries high risk in terms of possible terrorism or lone offenders. Illegal e-commerce, incl. the import of dangerous substances, are also increasing the likelihood of CBRNe incidents. Relevant know-how and skills, technical ability, the availability of (personal protective) equipment, and specific vehicles (incl. in the area of explosive ordnance disposal) are also crucial. It is closely related to protection of citizens and infrastructure, crisis management and strategic communication. There were many similar actions carried out from 2014-2020 ISF programme (e.g purchasing bomb robots and bomb suits) which have had a major positive impact in the field.

ISF 2014-2020 supported the **updating of the system of early warning** in case of danger of radiation (caused by man-made crisis, e.g. a dirty bomb). It is planned to further upgrade this system and include new functionalities like the analysis of radioactive noble gases.

One area where Estonia plans to contribute more in the near future is the wider and more systematic use of **drones in the fight against crime**. This would considerably improve the capacity to detect and react to security incidents and contributes to the protection of people and public spaces. This also supports the police in enhancing cooperation with European Union law enforcement agencies in the fight against serious and organized crime.

Measures for **physical protection of security relevant infrastructure** and/or ensuring their resilience during crisis are crucial. The continuity of the activities of the Police and Border Guard Board, the Rescue Board or other institutions providing essential services in crisis situations must be ensured.
It is also important to enhance the **forensic capacity** to provide forensic expertise.

An indicative list of actions in connection with Annex III include:

- actions that improve resilience as regard emerging threats, including chemical, biological, radiological and nuclear threats;
- financing of equipment and communication systems.

Other actions within the scope of ISF may be considered during the implementation of the programme, depending on the needs and available resources.

Operating support:

Estonia plans to use operating support to better contribute to the achievement of the objectives of the ISF programme. The use of operating support enables to maintain capabilities which are crucial to the Union as a whole.

There is a need to increase the number of staff in the Central Criminal Police Cybercrime Bureau to improve the capacity to collect and analyse the information. Staff costs will be covered by using the operating support. The final beneficiary is the Police and Border Guard Board which is by the statute responsible for security and public order in the state and the investigation and prevention of offences.

Financial instruments: n/a.

2.3.2 Indicators

Reference: Article 22(4)(e) CPR

Table 7: Output indicators					
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Milestone (2024)**	**Target (2029)**
SO3	***O.3.1***	***Number of participants in training activities***	***number***	***3 035***	***9016***
SO3	***O.3.2***	***Number of exchange programmes/workshops/study visits***	***number***	***28***	***63***
SO3	***O.3.3***	***Number of equipment items purchased***	***number***	***91***	***160***
SO3	***O.3.6***	***Number of projects to prevent crime***	***number***	***2***	***4***
SO3	***0.3.7***	***Number of projects to assist victims of crime***	***number***	***0***	***1***

Table 8: Result indicators										
Specific objective	**ID [5]**	**Indicator [255]**	**Measurement unit**	**Baseline or reference value**	**Baseline measurement unit**	**Reference year**	**Target (2029)**	***[Measurement unit for target]*** [1]	**Source of data [200]**	**Comments [200]**
SO3	*R.3.12*	*Number of participants who consider the training useful for their work*	*number*	*0*	*share*	*2021*	*4593*	*number*	*Project reports, participant feedback survey*	

[1] *The Council's partial mandate added this column.*

SO3	*R.3.13*	*Number of participants who report three months after leaving the training that they are using the skills and competences acquired during the training*	*number*	*0*	*share*	*2021*	*2 666*	*number*	*Project reports, participant feedback survey*	

2.3.3 Indicative breakdown of the programme resources (EU) by type of intervention

Reference: Article 22(5) CPR and Article 13(18) of the BMVI Regulation or Article 13(12) ISF Regulation or Article 16(12) AMIF Regulation

Table 9

Specific objective	Type of intervention	Code	Indicative amount (Euro) EU contribution
SO3	IT-systems, interoperability, data quality, communication systems (excluding equipment)	001	1 117 500
SO3	Training	005	2 150 068.9
SO3	Exchange of best practices, workshops, conferences, events, awareness raising campaigns, communication activities	006	715 375
SO3	Studies, pilot projects, risk assessments	007	684 250
SO3	Equipment	008	8 407 875

2.4 Technical assistance

Reference: Article 22 (3)(f); Article 36 (5) CPR; Article 37 CPR; Article 95 CPR;

Technical assistance is the precondition that sufficient means and resources are available to achieve the objectives and indicators set in the ISFprogramme.

TA is used for

- Preparation, implementation, monitoring and control
- Capacity building
- Evaluation and studies, data collection
- Information and communication

Preparation, implementation, monitoring and control

TA is used by the competent officials of Responsible Authority (RA) and Audit Authority (AA). In the Ministry of the Interior there are approximately 10 RA officials responsible for implementation of HOME funds and 2 AA auditors. The TA is used for the RA and AA personnel costs, training, participation in workshops and meetings, etc.

Capacity building

Consultation and sharing of best practices are key factors in successful implementation so that applicants and beneficiaries have the ability to prepare and implement projects. Therefore, the RA also ensures continuous training, counselling and guidance of applicants and beneficiaries funded by the TA.

To reduce the burden on applicants and beneficiaries, the TA is used for novel IT solutions of application, reporting and reimbursement. The SFOS information system will be introduced to simplify the technical procedures, reduce the workload of applicants, beneficiaries and administration, and thus contribute more to substantive activities. The principle of single entry is used as far as possible for electronic applications. In addition, the information system enables the RA to monitor the achievement of results, the progress of commitments and disbursements,

the volumes and results of audits, administrative, financial and on-the-spot controls, irregularities and recoveries.

Evaluation and studies, data collection

It is important to ensure that objectives are met in time and resources are used efficiently. Therefore two evaluations are foreseen: the mid-term evaluation in 2024 and final evaluation in 2030. If needed, resources could be used for studies and data collection.

Information and communication

The TA is also used for communication and publication activities (see p 7.)

Text field [3000] (Technical assistance pursuant to Article 37 CPR)

Estonia is not planning to use technical assistance not linked to costs.

Table *10*

Type of intervention	Code	Indicative amount (Euro)
Information and communication	001	32 348,44
Preparation, implementation, monitoring and control	002	1 471 853,59
Evaluation and studies, data collection	003	48 522,65
Capacity building	004	64 696,86

3. Financial plan

Reference: Article 17(3)(f)

3.1. Financial appropriations by year (this table is not filled in SFC)

Table 11: ***Financial appropriations by year***								
Fund	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
ISF								

3.2 Total financial allocations

Table *12: Total financial allocations by fund and national contribution*

				Indicative breakdown of national contribution				
Specific objective (SO)	**Type of action**	**Basis for calculation Union support (total or public)**	**Union contribution (a)**	**National contribution (b)=(c)+(d)**	**Public (c)**	**Private (d)**	**Total (e)=(a)+(b)**	**Co-financing rate (f)=(a)/(e)**
1. Exchange of information	Regular actions	Total	3,822,305.25	1,274,101.75	1,274,101.75	0.00	5,096,407.00	75.0000000000%
1. Exchange of information	Annex IV actions	Total	4,321,959.00	1,440,653.00	1,440,653.00	0.00	5,762,612.00	75.0000000000%
1. Exchange of information	Operating support	Total	3,980,291.41	1,326,763.90	1,326,763.90	0.00	5,307,055.31	74.9999986339%
Total Exchange of information			**12,124,555.66**	**4,041,518.65**	**4,041,518.65**	**0.00**	**16,166,074.31**	**74.9999995515%**
2. Cross-border cooperation	Regular actions	Total	1,327,500.00	442,500.00	442,500.00	0.00	1,770,000.00	75.0000000000%
2. Cross-border cooperation	Specific actions	Total	429,901.20	47,766.80	47,766.80	0.00	477,668.00	90.0000000000%
2. Cross-border cooperation	Annex IV actions	Total	0.00	0.00	0.00	0.00	0.00	
Total Cross-border cooperation			**1,757,401.20**	**490,266.80**	**490,266.80**	**0.00**	**2,247,668.00**	**78.1877572666%**
3. Preventing and combating crime	Regular actions	Total	9,834,000.00	3,278,000.00	3,278,000.00	0.00	13,112,000.00	75.0000000000%
3. Preventing and combating crime	Specific actions	Total	436,068.90	48,452.10	48,452.10	0.00	484,521.00	90.0000000000%
3. Preventing and combating crime	Annex IV actions	Total	1,687,500.00	562,500.00	562,500.00	0.00	2,250,000.00	75.0000000000%
3. Preventing and combating crime	Operating support	Total	1,117,500.00	372,500.00	372,500.00	0.00	1,490,000.00	75.0000000000%
Total Preventing and combating crime			**13,075,068.90**	**4,261,452.10**	**4,261,452.10**	**0.00**	**17,336,521.00**	**75.4192199231%**
TA.36(5). Technical assistance - flat rate (Art. 36(5) CPR)			1,617,421.54				1,617,421.54	100.0000000000%
Grand total			**28,574,447.30**	**8,793,237.55**	**8,793,237.55**	**0.00**	**37,367,684.85**	**76.4683373206%**

Table 13 Transfers between shared management funds*

No transfers from ISF to other funds of from other funds to ISF are foreseen

Receiving fund / instrument / *Transferring fund / Instrument*	*AMIF*	*ISF*	*BMVI*	*ERDF*	*ESF+*	*CF*	*EMFF*	*Total*
AMIF		*N/A*	-	-	-	-	-	-
ISF	*N/A*		-	-	-	-	-	-
BMVI	-	-		-	-	-	-	-
Total	-	-	-	-	-	-	-	-

** Cumulative amounts for all transfers during programming period.*

[Table 9 Transfers to instruments under direct or indirect management]*	*Transfer amount*
Instrument 1[name]	*N/A*
Instrument 2[name]	
Total	

** Cumulative amounts for all transfers during programming period*

4. Enabling conditions

Reference: Article 17(3)(h)

Table *14*					
Enabling condition	**Fulfilment of enabling condition**	**Criteria**	**Fulfilment of criteria**	**Reference to relevant documents**	**Justification**
Effective monitoring mechanisms of the public procurement market	*YES*	Monitoring mechanisms are in place that cover all public contracts and their procurement under the Funds in line with EU procurement legislation. This requirement includes: 1. Arrangements to ensure compilation of effective and reliable data on public procurement procedures above the EU thresholds in accordance with reporting obligations under Article 83 and 84 of Directive 2014/24/EU and Article 99 and 100 of Directive 2014/25/EU. 2. Arrangements to ensure the data cover at least the following elements: a. Quality and intensity of competition: names of	YES	Public Procurement Register (https://riigihanked.riik.ee) Public Procurement Act (https://www.riigiteataja.ee/en/eli/505092017003/consolide) Competition Act (https://www.riigiteataja.ee/en/eli/517062021003/consolide) Information from the Ministry of Finance (https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigihangetepoliitika/kasulikteave/riigihankemaastikukokkuvotted; https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigihangetepoliitika/kontaktid)	Public contracts above the national threshold and procurement under EU procurement law are published and executed on the central e-procurement portal "Public Procurement Register" managed by the Ministry of Finance (MoF) in accordance with Reg (EU) 2015/1986. MoF is responsible for monitoring, reporting and consulting pursuant to Art 83 and 84 of EU 2014/24 and Art 99 and 100 of EU 2014/25. Monitoring and reporting are based on data retrieved from the Central Public Procurement Register. a. the names of the successful tenderers, the indicative number of tenderers and the contract value shall be published in the public procurement register in the form of a contract award notice in accordance with Commission Reg EU 2015/1986. b. After completion of procurement, the contracting authority will publish the contract-specific information on the final price in the public procurement register.

		winning bidder, number of initial bidders and contractual value; b. Information on final price after completion and on participation of SMEs as direct bidders, where national systems provide such information. 3. Arrangements to ensure monitoring and analysis of the data by the competent national authorities in accordance with Article 83 (2) of Directive 2014/24/EU and Article 99(2) of Directive 2014/25/EU. 4. Arrangements to make the results of the analysis available to the public in accordance with article 83(3) of Directive 2014/24/EU and Article 99(3) Directive 2014/25/EU. 5. Arrangements to ensure that all information pointing to suspected bid-rigging situations is communicated to the competent national bodies in accordance with Article 83 (2) of Directive 2014/24/EU			Information on the participation of SMEs as direct tenderers is published in the scheme award notice – 100 % of e-procurement is carried out in a central procurement register. 3. The authority responsible for state supervision (monitoring) and analysis is the Ministry of Finance. Monitoring obligations are laid down in the Public Procurement Act. 4 people and one person are responsible for the overall analysis of public procurement data. 4. According to the Public Procurement Act § 180 p 7 Ministry of Finance submits once a year to the Government of the Republic an overview of the public procurement policymaking, advisory and training activities, state supervision and the activities of the public procurement register. The yearly overview is published at website of Ministry of Finance (https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigihangete-poliitika/kasulik-teave/riigihankemaastiku-kokkuvotted). According to PPA in case of a suspicion of an offence which has the characteristics of a possible case of corruption, the Ministry of Finance shall inform the investigating authority or the public prosecutor's office. The Competition Authority is also an investigating authority and administers supervision over implementation of Competition Act 54, it has to be informed about any offences of the competition regulation.

		and Article 99 (2) of Directive 2014/25/EU.Criterion 1			MOF webpage indicates that in case of doubt of possible anti-competitive co-operation, the Competition Authority has to be informed.
Effective application and implement ation of the EU Charter of Fundament al Rights	*YES*	Effective mechanisms are in place to ensure compliance with the EU Charter of Fundamental Rights which include: 1.Arrangements to ensure compliance of the programmes supported by the Funds and their implementation with the relevant provisions of the Charter. 2.Reporting arrangements to the monitoring committee on the cases regarding non-compliance of operations supported by the Funds with the Charter.	YES	UN, Common core document forming part of the reports of States parties – Estonia https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=HRI%2fCORE%2fEST%2f2015&Lang=en Estonian Constitution https://www.riigiteataja.ee/en/eli/ee/521052015001/consolide/current The Gender Equality and Equal Treatment Commissioner http://www.vordoigusvolinik.ee/?lang=en Gender Equality Act https://www.riigiteataja.ee/en/eli/530102013038/consolide Equal Treatment Act https://www.riigiteataja.ee/en/eli/530102013066/consolide The Legal Information Centre for Human Rights http://www.lichr.ee/home/?lang=en	EU Charter is respected in strategies, development plans, project selection criteria and measure-specific acts. The institutions involved in the protection of FR are members of monitoring committee and involved in monitoring and implementation of the ISF. The selection criteria for projects include the horizontal principles set out in Art 9 of CPR. Applicants and beneficiaries are guided how to respect the principles of the EU Charter. Monitoring committee (MC) consists of partners who monitor compliance with the Charter and present a consolidated vision and, where appropriate, problems in their field to the MC eg Gender Equality and Equal Treatment Commissioner, EE Chamber of Disability, Chancellor of Justice, etc.). MC members will be able to open the debate or to add the points to the agenda of the MC agenda in case the activities supported by ISF do not comply with the Charter, including in case of any doubt that, despite all the procedural requirements in place, there may be non-compliance with the Charter.

Implementation and application of the United Nations Convention on the rights of persons with disabilities (UNCRPD) in accordance with Council Decision 2010/48/EC	*YES*	A national framework to ensure implementation of the UNCRPD is in place that includes: 1. Objectives with measurable goals, data collection and monitoring mechanisms. 2. Arrangements to ensure that accessibility policy, legislation and standards are properly reflected in the preparation and implementation of the programmes.	YES	Welfare Development Plan 2016-2023 https://www.sm.ee/et/heaolu-arengukava-2016-2023 Accessibility Council https://www.riigikantselei.ee/et/ligipaasetavuse-rakkeruhm Chancellor of Justice Act(https://www.riigiteataja.ee/akt/12788991?leiaKehtiv Detailed requirements for buildings related to the special needs of persons with disabilities(https://www.riigiteataja.ee/akt/131052018055 Requirements set on living space[2] https://www.riigiteataja.ee/akt/103072015034?leiaKehtiv	Welfare Development Plan sets policy to protect the rights of persons with disabilities and describes challenges and indicators. The Social Security Programme provides solutions to modernise disability benefits and services system. The Care Programme focuses on improving access to and quality of social services, developing services that involve people in society and protecting fundamental rights. Statistics on the situation of persons with disabilities are collected by Statistics Estonia. The Ministry of Social Affairs publishes regular statistics and carries out studies. A comprehensive accessibility policy was developed in 2019 by Government's Task Force on Accessibility. The Ministry of Social Affairs is the national coordinator and promoter of accessibility for all sectors: supporting the work of the Accessibility Council, commissioning analyses and studies, coordinating the transposition of the Accessibility Directive (EU) 2019/882.The Equality Competence Centre provides advice and monitors compliance with requirements of accessibility and equal opportunities. Chancellor of Justice and Disability Council (DC) promote, protect and monitor the implementation of the CRPD. DC works on the basis of Article 33(3) of the UN

[2] Unofficial translation

					Convention on the Rights of Persons with Disabilities. MC members will be able to open the debate by e-mail or to add the points to the agenda of the MC meeting should there be a case in which the activities supported by ISF do not comply with the UN Convention on the Rights of Persons with Disabilities.

5. Programme authorities

Reference: Article 17(3)(j), Article 65 and 78 CPR

Table *15*	**Name of the institution** [500]	**Contact name and position** [200]	**e-mail [200]**
Managing authority	Estonian Ministry of the Interior	Tarmo Miilits, Secretary General	info@siseministeerium.ee
Audit authority	Internal Audit Department of the Estonian Ministry of the Interior	Tarmo Olgo, Head of the Internal Audit Department	tarmo.olgo@siseministeerium.ee
Body which receives payments from the Commission	Ministry of Finance	Marge Kaljas, Adviser of the Treasury Department	marge.kaljas@fin.ee

6. Partnership

Reference: Article 17(3)(g) CPR;

The preparation of the ISF programme is based on the principle of openness. All relevant stakeholders were given an opportunity to contribute to resolving Estonia's current and future challenges in implementing internal security policy.

In Estonia, the strategic planning of the national needs and their financing is centralized. There is no separate process (incl. involvement of partners and stakeholders) for programming the EU funds. The planning is source-neutral; the mapping of important strategic goals is done in the process of developing national strategies.

The ISF programme for 2021-2027 has planned hand in hand with preparing the long-term national umbrella strategy "Estonia 2035" and the "Internal Security Development Plan". An overview of compiling the strategies is found on following websites: https://www.riigikantselei.ee/et/Eesti2035 and https://www.siseministeerium.ee/et/STAK2030.

The process started in the spring of 2018. At the end of 2018 and the beginning of 2019, consultations with other ministries and umbrella organizations took place. Additionally, discussions were held in all counties. County Security Councils, other institutions related to internal security in the county, interest groups and representatives of civil society organizations, city and rural municipality leaders, and the county development centers were invited to the discussions. In total, more than 100 stakeholders contributed to preparing the long-term strategy. The discussions were summarized and used in the preparation of the "Internal Security Development Plan 2020–2030".

The development plan was submitted for public consultation through the dedicated web platform. The same system was used to get an approval from all ministries and the Government Office, and an opinion of the Association of Estonian Cities and Municipalities.

The financing for meeting the goals set in strategies are decided during the annual discussions of national budget, which guarantees synergy with national and other resources and enables to avoid double financing.

The implementation of the Internal Security Development Plan is monitored by the sectoral committee which consists of representatives from relevant authorities, intermediate bodies and partners.

There is a common committee to monitor the implementation of the BMVI, ISF and AMIF. This monitoring committee consists of the same parties which are members of the sectoral committees of the Internal Security Development Plan. In addition, bodies responsible for promoting social inclusion, fundamental rights, rights of persons with disabilities, gender equality and non-discrimination are involved.

7. Communication and visibility

Reference: Article 17(3)(i) CPR, Article 42(2) CPR

The communication of EU funds aims to ensure target group awareness of EU support through comprehensive, open and relevant communication.

A single website portal providing access to all programmes covered by CPR will be established by the State Shared Service Centre (SSSC). In addition to the Estonian language, the website portal will be made available in English and Russian as well, since surveys show that the Russian-speaking population is less aware of the support measures.

The Ministry of the Interior ensures the continuation of dedicated website for the HOME funds covering the programmes' objectives, activities, available funding opportunities and achievements. Estonia ensures transparency on the implementation of the national programme and publishes a list of actions supported by each programme.

Both, the single website portal as well as HOME funds website are designed and constructed to comply with the WCAG 2.0 AA Accessibility Guidelines. This means that certain technical tools and content creation principles have been used to help consumers with visual, hearing, physical, speech, cognitive, language, learning, and neurological disabilities use the content of the website.

A Facebook page is used to communicate HOME funds' calls for proposals and achievements of projects.

The communication coordinator in the SSSC will lead the national communication network to ensure central visibility, transparency and communication activities. Furthermore, it will hold a yearly national Europe Day in association with the European Commission Representation in Estonia.

A dedicated HOME funds communication officer is appointed within the Ministry of the Interior.

Technical Assistance is used for communication activities.

Indicators:

1. Audio storytelling through five (5) podcasts to rise awareness of the projects financed from the HOME funds during the new period. Podcasts will be part of the regular podcasts published by the Ministry of the Interior.
2. At least four (4) major information activities during the new period to present the achievements for the target audience.
3. At least four (4) digital media content created, including visual content such as illustrations and video materials to introduce the HOME funds in Estonia.
4. New social media channels (Facebook, Youtube) developed for the Home funds in Estonia to reach out to a wider audience. Creating new content and cross-referencing on other similar social media accounts to grow following.