**EN**

**This action is funded by the European Union**

Annex I

to the Commission Implementing Decision on the Annual action plan in favour of North Macedonia for 2024

Action Document for EU for Enhanced Security

**Annual Action plan**

This document constitutes the annual work programme in the sense of Article 110(2) of the Financial Regulation, and annual and multiannual action plans and measures in the sense of Article 9 of IPA III Regulation and Article 23 of NDICI - Global Europe Regulation.

# SYNOPSIS

# Action Summary Table[[1]](#footnote-2)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | EU for Enhanced Security  Annual action plan in favour of North Macedonia 2024 | | | | |
| **OPSYS** | [/OPSYS business reference][[2]](#footnote-3): <reference> | | | | |
| **ABAC** | ABAC Commitment level 1 number: <reference> | | | | |
| **Basic Act** | Financed under the Instrument for Pre-accession Assistance (IPA III) | | | | |
| **Economic and Investment Plan (EIP)** | Yes | | | | |
| **EIP Flagship** | Yes  Priority Area: “Rule of law, governance and Public administration reform” – 100% | | | | |
| **Team Europe[[3]](#footnote-4)** | No | | | | |
| **Beneficiar(y)/(ies) of the action** | The action shall be carried out in North Macedonia | | | | |
| **Programming document** | IPA III Programming Framework | | | | |
| **PRIORITY AREAS AND SECTOR INFORMATION** | | | | | |
| **Window and thematic priority[[4]](#footnote-5)** | Window 1: Rule of law, fundamental rights and democracy  Thematic Priority 3 Fight against organised crime/security (100 %) | | | | |
| **Sustainable Development Goals (SDGs)** | Main SDG 16: Peace, Justice and Strong Institutions | | | | |
| **DAC code(s)**[[5]](#footnote-6) | 15210 - Security system management and reform | | | | |
| **Main Delivery Channel** | 12000-Recipient Government | | | | |
| **Targets** | Climate  Gender  Biodiversity | | | | |
| **Markers[[6]](#footnote-7)**  **(from DAC form)** | **General policy objective** | **Not targeted** | **Significant objective** | | **Principal objective** |
| Participation development/good governance |  |  | |  |
| Aid to environment |  |  | |  |
| Gender equality and women’s and girl’s empowerment |  |  | |  |
| Reproductive, maternal, new-born and child health |  |  | |  |
| Disaster Risk Reduction |  |  | |  |
| |  | | --- | | Inclusion of persons with  Disabilities | |  |  | |  |
| Nutrition[[7]](#footnote-8) |  |  | |  |
| **RIO Convention markers** | **Not targeted** | **Significant objective** | | **Principal objective** |
| Biological diversity |  |  | |  |
| Combat desertification |  |  | |  |
| Climate change mitigation |  |  | |  |
| Climate change adaptation |  |  | |  |
| **Internal markers[[8]](#footnote-9) and Tags** | **Policy objectives** | **Not targeted** | **Significant objective** | | **Principal objective** |
| EIP |  |  | |  |
| EIP Flagship | YES  ☐ | | NO | |
| Tags[[9]](#footnote-10): | YES | | NO | |
| Transport |  | |  | |
| Energy |  | |  | |
| Environment and climate resilience |  | |  | |
| Digital |  | |  | |
| Economic development (incl. private sector, trade and macroeconomic support) |  | |  | |
| Human Development (incl. human capital and youth) |  | |  | |
| Health resilience |  | |  | |
| Migration and mobility |  | |  | |
| Agriculture, food security and rural development |  | |  | |
| Rule of law, governance and Public Administration reform |  | |  | |
| Other |  | |  | |
| Digitalisation[[10]](#footnote-11) |  |  | |  |
| Tags[[11]](#footnote-12)  digital connectivity  digital governance  digital entrepreneurship  digital skills/literacy  digital services | YES | | NO | |
| Connectivity |  |  | |  |
| Tags  digital connectivity  energy  transport  health  education and research | YES | | NO | |
| Migration[[12]](#footnote-13) |  |  | |  |
| Reduction of Inequalities |  |  | |  |
| COVID-19 |  |  | |  |
| **BUDGET INFORMATION** | | | | | |
| **Amounts concerned** | Budget line: 15.020101.01  Total estimated cost: EUR 5 200 000  Total amount of EU budget contribution EUR 5 000 000 | | | | |
| **MANAGEMENT AND IMPLEMENTATION** | | | | | |
| **Implementation modalities (management mode and delivery methods)** | **Direct management** through:  - Grants, and  - Procurement | | | | |
| **Final Date for conclusion of Financing Agreement** | At the latest by 31 December 2025 | | | | |
| **Final date for concluding contribution / delegation agreements, procurement and grant contracts** | 3 years following the date of conclusion of the financing agreement, with the exception of cases listed under Article 114(2) of the Financial Regulation | | | | |
| **Indicative operational implementation period** | 72months following the conclusion of the Financing Agreement | | | | |
| **Final date for implementing the Financing Agreement** | 12 years following the conclusion of the Financing Agreement | | | | |

# Summary of the Action

The Action aims at enhancing the security architecture of North Macedonia by strengthening the country’s response to security threats and risks, posed by cyber-crime, organised crime, terrorism, radicalisation and violent extremism. This will be achieved through modernising the operational tools, practices and regulations, improving the coordination among the institutions, upgrading the forensic capacities and the capabilities of the police and law enforcement agencies to anticipate, prevent and combat crime in all forms and manage security-related incidents, risks and crises.

The Action will address the increasing risks of cyber-attacks and the theft of sensitive information. This is vital in the context of the country's global connectivity and the potential for malicious users and criminal organisations to exploit system vulnerabilities. The Action will establish a National Operational Centre to coordinate all cyber security activities, will develop national procedures and methodology, will upgrade the cyber security infrastructure and the national capacities for identifying, investigating, and preventing cyber incidents and cybercrime, and will support the country’s collaboration with dedicated regional, European and global cyber security networks.

The EU assistance will also allow North Macedonia to enhance the performance of the police and other law enforcement agencies to investigate and address crime in line with the international standards**.** The action will transfer good practices from the EU Member states to improve the institutional coordination, assess complex crime cases and factor the lessons learned in the national legislation and methodologies, promote pre-emptive, preventive, strategic and tactical approaches, refine and modernise the investigative methods and techniques, upgrade the forensic capacities, improve the skills, knowledge of anti-crime officers, improve data collection. It will also upgrade the capacities of the National Counter-Terrorism Action Team's and will apply innovative ways to cope with violent extremism and radicalisation in prisons.

By addressing these issues, North Macedonia will improve the security architecture and will create a safer environment for its citizens.

## Beneficiar(y)/(ies) of the Action

The Action shall be carried out in North Macedonia

# RATIONALE

# Context

# Cybersecurity

According to the 2020 International Communication Union (ITU) Global Cybersecurity Index (GCI), North Macedonia ranks 24th in Europe and 38th globally, scoring 89.92. This index measures the commitment of countries to cybersecurity at a global level to raise awareness of the importance and different dimensions of the issue and assess countries’ Information and Communication Technology (ICT) resilience and reliability. It highlighted the legal and cooperative measures as the country’s strength areas and the technical measures as an area of potential growth[[13]](#footnote-14).

North Macedonia is a member of the *Budapest Convention on Cybercrime* and participated in *Europol’s Analysis Projects in environmental crime and cybercrime*. The country is also active in all elements of cooperation in which Europol includes its external partners, including cybercrime, migrant smuggling and counterterrorism. From a legal point of view, the country does not have an overarching law on cybersecurity. However, the related set legislation in this field is the following: - *Law on Interception of Communication*; - *Law on Electronic Communications; - Law on e-Commerce; - Law on Electronic Management and Electronic Services; - Law on Data in Electronic Form and Electronic Signature; - Law on Personal Data Protection*; - *Law on the Security of Network and Information Systems;* and – *Law on Free Access to Public Information.*

North Macedonia adopted its Cybersecurity Strategy and a corresponding Action Plan 2018–2022 in 2018, with actions around five strategic objectives: cyber resilience; capacities and culture; combating cybercrime; cyber defence; and cooperation and information exchange. The strategy acknowledges alignment with the EU Cybersecurity Strategy and the NATO Cyber Defence Pledge. In substance, the strategy is rather generic, and the action plan only sets forth strategic priorities and start and end dates for each activity. It misses some rather fundamental cybersecurity aspects (legislation, competent authorities, cooperation framework and Critical Information Infrastructures CIIs) and lacks performance indicators to measure success. Importantly, the two key implementing bodies – the National Cyber Security Council and the Operational Implementation Body (OBCS or the Digital Agency) – have never fully materialised. With the strategy reaching the end of its validity period, a new working group has recently been set up by the Ministry of Information Society and Administration (MISA) to prepare a new National Cybersecurity Strategy. The working group consists of representatives from the Ministries of Defence, Interior, Information Society and Administration, Foreign Affairs, the Agency for Electronic Communications and the National Centre for Computer Incidents Response (MKD-CIRT).

In addition to the National Cybersecurity Strategy and its supporting documents, the cybersecurity prevention of the country is given a special place in the National Strategy on Building Resilience and Confronting Hybrid Threats 2021-2025, adopted on 5 October 2021. This aspect is intertwined in almost all of the main areas identified in this document, which are the political sector, economy, defence sector, civil sector, infrastructure and the ICT domain. This strategy recognizes that North Macedonia as a NATO member country has its own obligations to work on building resilience of its society, and adds that the development of this strategy has been also initiated by the EEAS in 2019 and is in accordance with the common EU framework for hybrid threats prevention of 2016.

The government is also recognising disinformation as a kind of cyber-threat and in 2019 it proposed a draft Action Plan against Disinformation. This plan has two main parts, security measures (which foresees a few actions of cyber protection and prevention in their nature) and pro-active measures.

MKD-CIRT, which operates within the Agency for Electronic Communications, was established in 2016 and has been assigned, in accordance with the Law, as the official national point of contact and coordination in dealing with security incidents in networks and information systems. To date, though, it cannot perform all the necessary tasks, including those expected and required by the EU Network and Information Security Directive (NIS), due to both the lack of a comprehensive legal framework and capacity. MKD-CIRT is understaffed), while the needs are greater. The Agency for Electronic Communications is in charge of security and integrity of public electronic communications networks and services in the country.

MKD-CIRT organises awareness raising activities on cybersecurity with state institutions. However, most of the websites and databases of the state institutions remain poorly maintained and highly vulnerable to small-scale cyber-attacks. Several cases have been reported by the media in which the institutional websites have underperformed on safety and security tests. In the coming period they plan to create activities involving private companies. MKD-CIRT is also conducting general awareness raising campaigns on social networks and in the media.

The Government recognises that several measures were taken to ensure proper capacity building and raising awareness in cybersecurity. These included incorporating content on safe internet in the primary education curriculum and developing information security-focused programmes for certain bachelor’s and master’s degrees to meet the demand for cybersecurity professionals[[14]](#footnote-15). Despite these efforts, 2020 was marked by massive cyber-attacks on governmental networks and entities, demonstrating a need for additional improvements in national cyber defence capacity, including relevant infrastructure. The European Commission also recognised in its Annual report 2021 that the implementation of the legal and strategic documents, requires additional efforts.

The very poor capacities of MISA, as the main ministry responsible for policy creation and coordination of cooperation between the institutions with regard to electronic communications (Chapter 10), represent a significant challenge.

There is a need of a more proactive participation of domestic institutions in the European networks, such as [ENISA](https://www.enisa.europa.eu/) (the European Union Agency for Cybersecurity), [the CSIRTs Network (Computer Security Incident Response Team network composed of EU Member States’ appointed CSIRTs and CERT-EU etc.](https://csirtsnetwork.eu/)

The Ministry of the Interior has cyber-related tasks mainly focused on internal security and the fight against cybercrime, but it also has a Sector for Computer Crime and Digital Forensics responsible for cybercrime investigations and matters related to electronic evidence, including digital forensics. The Ministry of Interior participates in the drafting of cybersecurity strategies and is additionally working with a complementing cybercrime strategy addressing the needs and objectives of law enforcement.

The Ministry of Defence is a key stakeholder in the cybersecurity strategy process and, together with the Military Academy, is also responsible for training and education. A very specific aim in the Action Plan of the National Strategy on Building Resilience and Confronting Hybrid Threat is establishing further cooperation with NATO and the EU on dealing with hybrid threats, for which the Army and the MD are in charge.

North Macedonia lacks official cybersecurity cooperation formats with the private sector and/or civil society organisations. Existing informal public-private consultations tend to be unstructured, irregular in character and formed on an ad hoc basis.

Cybersecurity is one segment of the digital transformation and it is closely linked to critical infrastructure development, digital skills, e-government services, respect of personal data protection, etc. Therefore, there is a necessity of whole-of-government approach.

**Crime and terrorism**

Regarding the fight against organised crime and terrorism, the necessary legal framework has been put in place through the amendments of the 2016 Criminal Code and the adoption of over 30 different laws, which are in line with European standards and criminalises trafficking in human beings, online child pornography, computer crime and drug trafficking. On the strategic framework, the most recent strategies adopted by the Government are the *National Strategy for the Prevention of Money Laundering and Financing Terrorism 2021-2024*, the *National Strategy for Capacity Building for Financial Investigations and Property Confiscation 2021-2023*, and the *National Strategy for Combatting Trafficking in Human Beings and Illegal Migration 2021-2025*. North Macedonia also has a *National Strategy for Countering Terrorism 2018-2022* and a *Strategy for Countering Violent Extremism 2018-2022*, both with related action plans. A National Plan for reintegration, resocialisation and rehabilitation of foreign fighters returnees and members of their families (women and children) was adopted in June 2020 to implement the identified priorities for preventing violent extremism and radicalisation.

The process of preparing the two national strategies: the Strategy for the Prevention of Violent Extremism and the Strategy for the Fight against Terrorism for the period 2023-2027, with action plans for their implementation, is in its final stages.

The strategies are institutionally and organizationally linked, according to the four pillars of the global strategies of the United Nations and the European Union for the prevention of violent extremism and the fight against terrorism. The four pillars: prevention, protection, prosecution/enforcement and response are strategic priorities. The activities will be implemented by a large and diverse group of stakeholders, primarily ministries and other state institutions, and international organizations, civil society, religious communities, local self-government and the private sector will also be involved.

Key institutions in the fight against *organised crime* include specialised police units within the Ministry of Interior. In addition, there is a Financial Intelligence Unit under the Ministry of Finance that collects information and helps identify suspicious transactions. Financial Investigation units were also set up within the Customs Administration, the Financial Police and the Ministry of Interior. The institutional framework is completed with a comprehensive reform of the intelligence services. The National Security Agency (NSA) is designated as an independent state body without police powers. The technical conditions for the proper functioning of the system for the interception of communications have been improved. The new *Law on the Intelligence Agency* was adopted in January 2021 in order to complete the new security set-up. The Basic Public Prosecutor’s Office for Prosecuting Organized Crime and Corruption is a specialised Basic Public Prosecutor Office under the direct supervision of the Public Prosecutors Office of North Macedonia, having the competence to investigate, prosecute and bring to justice cases of corruption and organised crime. The Agency for Management of Confiscated Assets is the key authority in managing confiscated property in cases of organised crime and terrorism.

The Republic of North Macedonia is a credible partner in the fight against terrorism and a member of the Global Coalition to Defeat ISIS. In this respect, there is strong support for the role of NATO in the fight of the international community against terrorism.

The country signed and ratified all conventions for the fight against terrorism and terrorism-related protocols of the United Nations, including Resolution 2178 (2014) of the UN Security Council and the Council of Europe Convention on the Prevention of Terrorism.

In line with the commitments from the Joint Action Plan on Counter-Terrorism for the Western Balkan, the Government approved the National Plan on Reintegration, Resocialisation and Rehabilitation of returnees from foreign armies and their family members (women and children).

The Standard Operating Procedures on reintegration, resocialisation and rehabilitation of foreign fighters and their family members are aimed at putting into effect the procedure which is based on the fundamental values for the protection of human rights and freedoms, a whole-of-government approach, individual approach and treatment, and the principle of confidentiality.

Countering terrorism and violent extremism is a complex security issue that does not recognise borders, cultures, religious or ethnic groups. It is a phenomenon affecting all of us, and therefore an integrated response by all relevant institutions is required.

This phenomena is the foundation of the state's protection against terrorist acts, primarily because violent extremism and terrorism result from individual or collective processes of radicalisation that may be used as justification for violence used to achieve certain goals (political, ideological, social).

In Resolution 2178 (2014), the Security Council clearly explains the link between violent extremism and terrorism, highlighting the importance of taking measures in line with international norms, and recognises the need for prevention: "violent extremism, which may be conducive to terrorism," requires collective efforts, "including the prevention of radicalisation, recruitment and mobilisation of individuals into terrorist groups and their transformation into foreign terrorist fighters".

Therefore, strategic planning of measures and activities for countering terrorism leading to radicalisation and violent extremism is considered a top priority in building safe and resilient communities and ensuring fundamental values such as the rule of law, human rights and freedoms, citizen safety, cultural values and the inclusiveness of society.

Countering terrorism leading to radicalisation and violent extremism is one of the significant challenges requiring: knowledge, i.e., understanding of the phenomenon and recognising/identifying the risks and push and pull factors, knowledge of required action in the event of added risks that maximise the likelihood of radicalisation, and of the convenient measures for risk management.

North Macedonia participates in international police cooperation. Cooperation with Europol was established following the conclusion of a strategic agreement in 2007 and an operational agreement in 2011. There is operational cooperation in the fight against the trafficking of human beings, weapons, and drugs. A secure communication link for information exchange (SIENA) was established. North Macedonia participated in Europol’s Analysis Projects on environmental crime and cybercrime. The country is also active in all elements of cooperation (incl. in EMPACT) in which Europol includes its external partners, including in the areas of cybercrime, migrant smuggling and counterterrorism, as well as Europol’s reporting and operations. Cooperation between the country and the EU Agency for Law Enforcement Training (CEPOL) is well-established and based on a working arrangement.

The country is committed to fully implementing the bilateral Western Balkans Joint Action Plan on Counterterrorism, putting a particular focus on (i) strengthening counter-terrorism structures and strategies, including an improved threat assessment; (ii) stepping up efforts to prevent and counter violent extremism, as well as addressing the challenges posed by returning Foreign Terrorist Fighters and their families; and (iii) establishing a national threat assessment of money laundering risks and improve the link between financial intelligence and prosecution.

In the fight against *terrorism*, there is a national coordinator for counter-terrorism and countering violent extremism. The Office coordinates inter-institutional cooperation through the National Committee for the Prevention of Violent Extremism and the Fight against Terrorism, chaired by the National Coordinator. The Committee includes representatives of the critical institutions countering terrorism and violent extremisms. Responsibility for terrorism-related issues is with the Ministry of Interior’s Department to suppress organised and serious crime.

The Action is designed to contribute to the achievement of the objectives of the **Joint Action Plan on Counterterrorism for the Western Balkans**[[15]](#footnote-16)**,** which establishes five objectives to be supported by the EU: 1. A robust framework for countering terrorism and preventing/countering violent extremism: institutional set-up and legal alignment, implementation and enforcement capacities; 2. Effective prevention and countering of violent extremism; 3. Effective information exchange and operational cooperation; 4. Build capacity to combat money laundering and terrorism financing; 5. Strengthen the protection of citizens and infrastructure.

The Action also aligns with the **Agreement on Operational and Strategic Cooperation with EUROPOL**, which aims to regulate the cooperation between Europol and North Macedonia in combating severe forms of international crime through exchanging information and regular contacts. It also contributes to implementing North Macedonia's agreement with EUROJUST which establishes a framework for structural judicial cooperation in the fight against serious cross-border crime between the EU Member States and North Macedonia. The agreement allows the partner States to participate in all the practical cooperation tools offered through Eurojust to prosecute severe, transnational crime cases.

More broadly, the Action will contribute to the regional **Southeast Europe 2020 Strategy, which aims** to establish a cross-border working group of border security agencies from Albania, Kosovo, North Macedonia, and Montenegro to combat corruption, illicit cross-border trafficking, transnational crime, and terrorism.

# Problem Analysis

Short problem analysis

***Cybersecurity***

Information and communication technologies (ICT) in North Macedonia have continuously increased in recent years. At the same time, this expansion is a primary driver of globalisation and contributes significantly to the development of the economy, living standards and the well-being of society. However, the increasing dependence on services provided in cyberspace means dysfunctional ICT systems and severe cyber-attacks can significantly negatively impact the functioning of the public and private sectors and society. Dependence on new technologies and the need for greater availability of services in cyberspace is a reason for users and institutions to increase awareness of the importance of data integrity, authenticity and confidentiality. Macedonian communication networks are part of the global communication networks, which means that cyber security incidents elsewhere can affect North Macedonian cyberspace and services, and *vice versa*.

Global connectivity can provide complete anonymity, increasing malicious users' ability to access, steal and misuse sensitive information. Globalisation and anonymity enable malicious users to carry out easier attacks on pre-defined victims and much more extensive operations and attacks on a much larger scale. Strengthening national capacities for dealing with cyber threats and improving cyber security at the national level are important for North Macedonia.

Cybercrime can appear as abuse and scams on the Internet and attacks on more sophisticated and complex systems. In this way, cybercrime can be motivated by different causes and carried out by various agents. Given the wide range of cybercrimes and the scope of the institutions and organisations in charge of the management and handling of cybercrime, this objective requires establishing a detailed and specialised national plan for the management of cybercrime, including crime enabled in cyberspace. This plan should define the cybercrime problem and the challenges it creates. It requires defining prevention activities and ensuring vital functions for society. The most efficient way of prevention is to provide proper instructions and solutions so that cyber hygiene can become an integral part of the culture and mentality of Macedonian society. Inter-agency and multi-disciplinary approaches are essential to address cybercrime efficiently.

The public and private sectors need to employ timely and accurate information and suggestions for cyber security and also to be able to cooperate in case of cyber incidents. In this manner, it is necessary to identify all relevant capacities for cyber security across all relevant stakeholders and define specific jurisdictions and activities to improve cyber safety and manage cyber incidents. The end goal is to secure the protection of an integral part of the infrastructure in the country and for relevant institutions to use adequate solutions in defending the state interests, thereby demonstrating readiness for severe, complex cyber threats.

The present Action will strengthen the capacities of law enforcement agencies to counter cybercrime and improve national cybersecurity.

***Crime and terrorism***

North Macedonia is investing significant efforts and resources in fighting organised crime, which threatens the security of the people, economic development, the rule of law and democracy. Both in the field of organised crime and the fight against terrorism, the country has experienced improvements in the track record of investigations, prosecutions and convictions and the exchange of information with the relevant institutions, including Europol. Likewise, local mechanisms for preventing and countering violent extremism are in place. However, despite these apparent improvements, police action and its investigative techniques need continuous updating.

As *organised crime* is dynamic, flexible, increasingly internationally connected, and mostly invisible, often related to legal structures, fighting it requires a solid strategic vision, political consensus, regional cooperation, and considerable state investments. Furthermore, successfully organised crime investigations require more training and perseverance than investigations of conventional crimes. Interviews, informants, searches, surveillance and other special investigative techniques are needed to determine an enterprise's precise nature and scope so it may be defeated successfully.

Conventional policing is primarily reactive, meaning that police action generally responds to crimes after they have been committed and reported. The successful investigation of organised crime requires proactive approaches, typically based on criminal intelligence analysis. Organised criminal groups have committed many crimes that are not reported to authorities, so searches through financial records and interviews with informants, citizens, and surveillance activities are often required to determine whether a crime has occurred. The two general features of the proactive approach include gathering intelligence, followed by a criminal investigation. Intelligence gathering evaluates information, followed by analysis to support informed decision-making. In some jurisdictions, it is up to the law enforcement agencies to carry out intelligence gathering and analysis; in others, there are trained analysts who perform intelligence analysis, often involving financial and business records, individual background checks, reports from police surveillance or use of other special investigative techniques, interviews with informants, and related information. The investigation determines whether the intelligence gathering and analysis results can be connected to the criminal conduct of groups or networks.

The Action will strengthen the capacities of police and other law enforcement agencies, with a focus on upgrading the human resource management and retention policy and further developing the investigations capacities, particularly hybrid and organised crime investigations skills, with pre-emptive, preventive, strategic and tactical approaches.

The fight against *terrorism* and radicalisation is another major threat to security and democracy. In the current context of globalisation, further progress can only be achieved in this thematic priority with sustainable and well-developed regional/international cooperation. North Macedonia invests in this vital effort to improve its capacities and coordination at the state and international levels through specific strategies and specialised bodies such as the National Committee for Countering Violent Extremism and Countering Terrorism.

The proposed Action will improve the capacities of law enforcement agencies to counter transnational organised crime and terrorism threats through enhancing abilities and cooperation in anti-terrorisms, implementation of national counter-terrorism and counter hybrid threat exercises to assess the functionality, proactiveness and efficiency of the National Counter Terrorism Action Team to coordinate all the institutional agencies and non-governmental bodies in tackling national and transnational terrorism threats and addressing the issue of violent extremism and radicalisation in prisons, (also involving reintegration and resocialisation of former prisoners).

Main stakeholders

* The **Ministry of Defence** (MD) isresponsible for implementing the Cyber Defence Strategythat differs from cybersecurity mainly in the nature and severity of cyber-attacks, with no opportunity to define precise criteria.
* The **Ministry of Interior (MoI)** is the leading policymaker in the home affairs sector, also responsible for coordinating and supervising the implementation and reporting of the sector reforms. Overall, the MoI plays a crucial role in ensuring the safety and security of citizens. Its diverse competencies cover a wide range of public safety and security areas.
* The **Cybercrime and Digital Forensic Sector of the Ministry of Interior.** This Unit investigates with the support of the CIRT. This Unit resulted from merging the Cybercrime Unit within the Department for Suppression of Organised and Serious Crime with the Forensic Department of the Ministry of Interior, intending to improve efficiency and effectiveness.
* The **Ministry of Information Society and Administration (MISA)** is the specialised government body for coordinating the activities for developing information society as listed mainly in the Strategic Plan of MISA and the Public Administration Reform Strategy and Action Plan 2018-2022.
* The **National Cyber Security Council** was established in July 2020 by the National Computer Security Strategy 2018-2022. This Council comprises the ministries of defence, interior and information society and administration. Its main functions are the following: -monitoring and coordinating the implementation of the National Cyber Security Strategy; -identifying the challenges of managing cyber crises and suggesting adequate measures for greater efficiency; -developing programmes and action plans for activities in the field of cyber security to be implemented by the Body with operation cyber security capacities**.**
* **The National Centre for Computer Incidents Response (MKD-CIRT).** According to Article 26 of the *Law on Electronic Communications*, the National Centre (MKD-CIRT) is set up within the Agency for Electronic Communications as a separate organisational unit, as the official national point of contact and coordination in dealing with security incidents in networks and information systems, and that will identify and provide a response to security incidents and risks.
* The **Public Security Bureau (PSB)** within the MoI comprises a set of structures responsible for ensuring public order and security, including combating organised crime, financial crimes, trafficking in human beings, drugs, weapons, terrorism cases and criminal intelligence and analysis.
* Concerning the fight against organised crime, the institutional framework has been under optimisation since 2018, when a major functional reform was launched. Three new bodies were established: **National Security Agency, Intelligence Agency and Military Agency**.
* An important vector of further development implies strengthening the national capacities for conducting financial and complex investigations and property confiscation. The PPO uses existing investigative capacities of the law enforcement agencies: **Financial Police, the Department for the Suppression of Organised and Serious Crime within MoI and Department for Criminal Police within MoI.**
* The **Institute of Forensic Medicine, Criminalistics and Medical Deontology, Medical Faculty**, within the University of St. Cyril and Methodius, is the highest-ranking institution in forensic expertise in North Macedonia. As a leading authority in this area of expertise, it is constantly upgrading its capacity and knowledge in the field of forensic sciences. Besides the scientific activities of the Institute, the core role of the Institute are the forensic laboratories dealing with the examination of evidentiary material and reporting findings to a responsible requesting institution (court/police/private person).

# Lessons Learned

The total IPA II envelope for home affairs for North Macedonia under the bilateral pillar reached almost EUR 30 million and covers the fight against organised crime, terrorism and money laundering, and border management, including quality of customs controls. The EU assistance in the area of cybersecurity has been channelled primarily through the multi-country 2019 project “EU support to cybersecurity capacity building in the Western Balkans”, involving Council of Europe, Member States, and the European Cybercrime Centre at Europol. The implementation of this essential country assistance provides for the formulation of the following lessons:

* The administrative and institutional capacity is a challenge as the role of national authorities for planning and implementing activities, and ensuring the effectiveness and sustainability of the EU assistance is vital. The massive staff turnover due to lack of merit-based approach and retention policy can be an obstacle in achieving progress or attaining results consolidation. To address this issue, North Macedonia is implementing a public administration reform, which still needs to deliver results. In parallel, mitigation measures such as strong capacity building at technical and managerial level and motivation building peer-to-peer are needed to ensure ownership and commitment.
* The coordination and cooperation between the various actors in the security area as well as the support from the society for the enforcement bodies are also important factors for fighting organised crime. Outreach approach to community needs to be paired with joint exercises involving the relevant beneficiaries to build trust and ensure supportive attitude.
* Organised crime is often cross-border, dynamic, well-digitalised, well-organised, and potentially infiltrating all decision-making systems. Therefore, fighting it successfully at the national level is practically impossible. Cooperation at the regional level, as well as with the EU structures, is, therefore, a must. National capacities must be available to allow the countries to exchange data and information and participate in joint repressive actions against organised criminal groups. A mix of regional and national tools can be more effective.
* The fight against organised and cross-border crime is a susceptible area which requires high-level political commitment. An inclusive sector policy dialogue must support this commitment and ownership. The low effectiveness of the governance and the institutions are also significant factors contributing to the success of organised crime. Therefore, well-working strategies involve a mix of tools. Capacity building will undoubtedly help a proactive approach from law enforcement; a combination of evidence from different sources will help the investigation processes decrease the pressure on the criminal groups; asset seizure is often more harmful to criminal groups than imprisonment. While digitalisation cannot be a panacea in the fight against organised crime, the technology leapfrogging may considerably improve how institutions operate and communicate, improve their performance, and reduce costs and delays in treating evidence.
* The criminal-justice approach must be coupled with solid prevention and awareness-raising approaches. This implies addressing the socio-economic factors that marginalise and enlarge the social basis for organised criminal groups. Therefore, the EU must invest equally in socio-economic development, focusing on education, the labour market and creating economic perspectives.

# DESCRIPTION OF THE ACTION

# Intervention Logic

The **Overall Objective** **(Impact)** of this Action is:

*To improve the security architecture of North Macedonia.*

The **Specific Objective (Outcome)** of this Action is:

*To strengthen the state response to security threats and risks, posed by cyber-crime, organised crime, terrorism, radicalisation and violent extremism.*

This Outcome will be achieved through the delivery of the following outputs:

***Output 1.1*** *Introduced operational tools for improving cyber-security and resilience and responding effectively to cyber-attacks, challenges and risks*

***Output 1.2*** *Strengthened capabilities of the police and law enforcement agencies to combat and prevent crime, terrorism and radicalisation and manage security-related incidents, risks and crises*

# Indicative Activities

The Action will be implemented through the following main activities:

**Output 1.1 Introduced operational tools for strengthening cybersecurity and cyber resilience.**

The action will provide advisory and capacity building support from EU Member states, on peer-to-peer basis, encompassing**:**

* Establishment and building the capacity of a National Operational Centre to coordinate all cyber activities, including active cyber prevention and effective response to cyber threats.
* Development of national procedures to manage incidents in times of peace, crisis, and state of emergency and development of communication guidelines in cases of cyber incidents and establishing standards for public communication. The procedures will ensure efficient and effective intra-institutional cooperation, based on clear roles and engagement. Every institution will have a pre-defined role and will employ appropriate protocols and procedures for information exchange, communication, and coordination.
* Development of the methodological basis for cybersecurity prevention and reaction including instructions and guidelines in case of cyber incidents and cyber crises.
* Improving the existing and establishing new mechanisms and tools (hardware and software) for identifying, investigating, and preventing cybercrime and cyber incidents.
* Upgrading the national capacities for identifying, investigating, and preventing cyber incidents and cybercrime. Upgrade the equipment and upscale the forensic knowledge and hybrid investigations.
* Performing a national cyber risk assessment.
* Improving regional and international cooperation and information sharing formats to allow for a better understanding and response to the constantly changing threat environment, participating in and strengthening cooperation with dedicated European and global CSIRT and technical communities (TF-CSIRT, FIRST) and with international cooperation networks (e.g. ENISA, Council of Europe).
* Developing technical skills of cybersecurity experts of governmental agencies and critical service providers through technical cybersecurity exercise and organising tabletop exercise (TTX) for cybersecurity-related with national experience and needs.
* Developing training tools, methodology and programmes for improving the understanding of the public administration on cyber security and mainstreaming cybersecurity training through the public administration training platform and developing internal safe communications habits and protocols/ disabling access to unverified websites, software across all device the public administration is using- this with an aim to prevent the vulnerability of the system.
* Implementation of a domestic awareness raising and outreach campaigns on cyber security targeting political leaders and high-level government officials on digital literacy, enhancing the cooperation with civil society organisations and private sector, strengthening the cooperation with media and journalists. The activity includes also the publication of regular threat reports, and insight into cybersecurity trends and developments to support the private sector and individuals take measures to prevent incidents.

**Output 1.2 Strengthened performance of the police and other law enforcement agencies to investigate and address crime in line with the international standards.**

The action will transfer good practices from the EU Member states to support the fight with the organised crime and counter terrorism and radicalisation. More specifically, it will:

* Analyse the system of cooperation between institutions involved in the fight against organised crime, terrorism and money laundering, assess complex serious crimes, with the objective to strengthen and if necessary to refine the legal framework for joint investigations on potential threats involving more than one law enforcement agency, enlarge the number and scope of joint investigations and increase the transparency of joint investigations.
* Improve the investigation skills of the officers involved in criminal investigations, fight against organized crime, terrorism and money laundering; assess complex serious crimes and promote pre-emptive preventive, strategic and tactical approaches, refine and modernise the investigative methods and techniques (interviews, informants, searches, surveillance, and other special investigative techniques),
* Improve the skills, knowledge of police officers and their role in the implementation of preventative measures against terrorism and radicalisation.
* Enhance the cooperation with regional and international organisations in the fight against organised crime and countering terrorism and money laundering.
* Further strengthen the capacities of the National Committee for Countering Violent Extremism and Countering Terrorism by providing support in implementation of the new National Strategy for Countering Terrorism and Violent Extremism.
* Further strengthen the capabilities of the Ministry of Interior’s (MOI’s) “Terrorism and Violent Extremism” Sector to **combat and prevent crime, terrorism and radicalisation**, as well as manage security-related incidents, risks and crises.
* Improve data collection, operational cooperation and information exchange concerning intelligence, law enforcement and justice to enhance detection, prevention and investigation of criminal offences and conducting criminal intelligence operations.
* Develop and conduct national counterterrorism and counter-hybrid threat exercises to assess the National Counter-Terrorism Action Team's functionality, proactiveness and efficiency to coordinate all the institutional agencies and non-governmental bodies in tackling national and transnational terrorism threats.
* Enhance capacities and cooperation of law enforcement personnel to address the issue of violent extremism and radicalisation in prisons and at the same time support reintegration and resocialisation of former prisoners, with a special focus on gender aspect.
* Revise the existing procedures and methodologies with the objective to ensure an adequate response by the criminal justice system to the needs of girls, women and other vulnerable groups in their interactions with police, investigators, legal professionals, judicial staff and others involved in the judicial process.

# Mainstreaming

**Environmental Protection, Climate Change and Biodiversity**

This Action is not addressing environmental challenges directly but supports the rule of law framework by enhancing the capacities of the law enforcement services to counteract criminality and protect citizens’ security and public order. Moreover, cybercrime has the potential to provoke loss of control over critical equipment and warning systems and cause harm to human health and the environment through catastrophic spills, waste discharges and air emissions. These events can cause fires, explosions, and releases of hazardous materials resulting in significant body injury, property damage, environmental remediation expense, and liability claims. This Action will contribute to improving the risk control and management and prevention of harm on environment.

**Gender equality and empowerment of women and girls**

As per OECD Gender DAC codes identified in section 1.1, this action is labelled as G1[[16]](#footnote-17). The country has ratified the Istanbul Convention and has established the legal framework to ensure gender equality by adopting the Law on equal opportunities for women and men and the Law on prevention and protection from discrimination. The current legal framework prohibits discrimination based on gender and sexual orientation. The action will support the enforcement of the existing legislation. Research suggests that women are disproportionately the targets of organised crime and certain forms of cyber violence compared to men. By improving the country’s responses to cyber threats and organised crime, the Action will contribute to prevention of violence against women. It will also propose new approach for respectful treatment of girls, women and other vulnerable people in contact with the criminal justice system.

**Disability**

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D0 as the action has no direct impact on people with disabilities. However, the action will reinforce the rule of law framework, which will allow the implementation in practice of principle of non-discrimination of minorities and vulnerable groups.

**Civil Society Organisation**

This Action has been developed in an inclusive process that involves civil society as part of the established sectoral policy dialogue. This approach will also be applied in the implementation stage. Civil society organisations form part of the Sector Working Groups (SWGs), channelling policy dialogue on sector priorities, IPA programming and reporting. Civil society organisations will participate in implementing the whole Action and, particularly, in promoting the awareness on cyber crime.

# Risks and Assumptions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Risks** | **Likelihood**  **(High/**  **Medium/**  **Low)** | **Impact**  **(High/**  **Medium/**  **Low)** | **Mitigating measures** |
| People and the organisation | Lack of political will to continue implementation of the sensitive sector reforms | M | H | Dynamisation of the policy dialogue with institutions and authorities of North Macedonia through mainly the Sector Working Group, with strong ownership and leadership by the relevant Minister. The accession process provides a leverage tool in this process. |
| Planning, process and system | Weak administrative capacity: lack of adequate number and quality staffing, especially in relation to the cybersecurity field. | H | H | The ongoing Public Administration Reform (PAR) addresses this issue. However, parallel capacity building measures, primarily on peer-to-peer basis (also included in this action), will allow improving the personal efficiency and motivation of the available staff and the newcomers. |
| Planning, process and system | Insufficient coordination and cooperation among institutions and law enforcement bodies. | H | H | The action addresses this weaknesses directly by enhancing the coordination among the law enforcement bodies. In addition, at policy level, an important mitigation measure is the strengthening of the Sector Working Groups channelling the coordination and policy dialogue. In addition, at project level, the Steering Committee will involve the relevant stakeholders. |
| People and the organisation | Lack of interest of the private sector and Civil Society Organisations (CSOs) on activities related to the Action | M | M | Improved interaction with business associations and support structures (incubators, accelerators, information centres), as well as with the Resource centre for the civil society and CSOs networks within the established sector working group and through targeted meetings. |

**External Assumptions**

The following assumptions should hold true to guarantee the success of the intervention:

* Stable progress on the EU accession path to back up the cooperation with the EU on security resilience
* Stable political situation and consistent reform orientation of any new government.
* The level of trust in the institutions improves
* Relevant national strategic and regulatory frameworks in place.
* Improving coordination and cooperation between law enforcing agencies
* Public administration reform progresses well and adequate staff retention policy is put in place
* Interest on behalf of the EU Member states to support the reforms in the sector

# Indicative Logical Framework Matrix

| **Results** | **Results chain:**  **Main expected results** | **Indicators** | **Baselines**  **(values and years)** | **Targets**  **(values and years)** | **Sources of data** | **Assumptions** |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | To improve the security architecture of North Macedonia | Political Stability and Absence of Violence/Terrorism[[17]](#footnote-18) (as measured by the World Bank Worldwide Governance indicators)[[18]](#footnote-19) | 50.47 (2020) | ≥ 50 (2027) | World Bank | *Not applicable* |
| Crime rate (Crimes over population 100.000 inhabitants. Considered crimes: intentional homicide; -attempted intentional homicide; -assault; -kidnapping; -sexual violence; -rape; -robbery)[[19]](#footnote-20) | 38,10 (2017) | ≤ 30 (2027) | Eurostat |
| Delayed investigation rate[[20]](#footnote-21) | 40% (2019) | ≤ 20 %(2027) | PPO |
| **Outcome 1** | *Strengthened state response to security threats and risks, posed by cyber-crime, organised crime, terrorism, radicalisation and violent extremism.* | Level of trust in the police (EU Public Opinion)[[21]](#footnote-22) | 48% (2019) | ≥ 57% (2026) | Eurobarometer | Stable progress on the EU accession path to back up the cooperation with the EU on security resilience  Stable political situation and consistent reform orientation of any new government.  The level of trust in the institutions improves |
| Financial investigation rate (Proportion of person under financial investigation over persons investigated for organised crime)[[22]](#footnote-23) | 48  57/148 = 38.5%[[23]](#footnote-24) | ≥42% (2026) | Financial Police CIU |
| Financial Investigation Rate on OCC by the PPOOCC[[24]](#footnote-25) | 26/126 = 21% (2019) | ≥ 37% (2026) | Financial Police |
| Percentage of executed confiscation sentences since 2011 for crimes related to organized crime, money laundering, abuse official duty (cumulative indicator)[[25]](#footnote-26) | 50% (till 2019) | ≥ 75% (till 2026) | Agency for confiscation of assets |
| Number of Computer cybercrimes[[26]](#footnote-27) | 169 (2022) | ≥ 120 (2026) | European Commission’s Report on North Macedonia |
| **Output 1** | Introduced operational tools for improving cyber-security and resilience and responding effectively to cyber-attacks, challenges and risks | Number of national procedures for managing cyber incidents in times of peace, crisis, and state of emergency prepared and adopted | 0 (2022) | 1 (2026) | Progress Report  Project Report | Relevant national strategic and regulatory frameworks in place.  Improving coordination and cooperation between law enforcing agencies  Public administration reform progresses well and adequate staff retention policy is put in place  Interest on behalf of the EU Member states to support the reforms in the sector |
| Number of National operation centre established and operational | 0 (2022) | 1 (2026) | Progress Report  Project Report |
| Number of manuals for handling case of cyber threat and attack prepared and adopted | 0 (2022) | 1 (2026) | Progress Report  Project Report |
| Number of people (public administration) trained on cybersecurity (cumulative indicator) | 0 (2022) | ≥ 100 (2026) | Progress Report  Project Report |
| Number of tabletop exercises (TTX) for cybersecurity related with national experience and needs (cumulative indicator) | 0 (2022) | ≥ 2 (2026) | Progress Report  Project Report |
| Number of public awareness events organised on cybersecurity | 0 (2022) | ≥ 2 (2026) | Progress Report  Project Report |
| **Output 2** | Strengthened capabilities of the police and law enforcement agencies to combat and prevent crime, terrorism and radicalisation and manage security-related incidents, risks and crises | Number of additional cooperation protocols with regional and international organisations in the fight against organised crime related to the Internet prepared and adopted | 0 (2022) | ≥ 3 (2026) | Progress Report  Project Report |
| Number of national cooperation protocols on investigations against organised crime prepared and adopted | 0 (2022) | ≥ 3 (2026) | Progress Report  Project Report |
| Number of people trained on modern investigation techniques and methods including forensic skills for criminal investigations | 0 (2022) | ≥ 50 (2026) | Progress Report  Project Report |
| Number of protocols on conducting investigations against perpetrators of crimes related to youths and women prepared and adopted | 0 (2022) | ≥ 2 (2026) | Progress Report  Project Report |
| Number of law enforcement agents trained on modern counter terrorism and hybrid investigations skills, with pre-emptive, preventive, strategic and tactical approaches | 0 (2022) | ≥ 30 (2026) | Progress Report  Project Report |
| Number of tabletop exercises (TTX) for terrorism (cumulative indicator) | 0 (2022) | ≥ 2 (2026) | Progress Report  Project Report |
| Number of terrorists whose assets are frozen | 0 (2022) | ≥ 5 (2026) | Progress Report  Project Report |

# IMPLEMENTATION ARRANGEMENTS[[27]](#footnote-28)

# Financing Agreement

In order to implement this Action, it is envisaged to conclude a financing agreement with North Macedonia.

# Indicative Implementation Period

The indicative operational implementation period of this Action, during which the activities described in section 3 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of conclusion of the financing agreement.

Extensions of the implementation period may be agreed by the Commission’s responsible authorising officer by amending this Financing Decision and the relevant contracts and agreements.

# Implementation Modalities

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[[28]](#footnote-29).

# Direct Management (Grants)

# *Grant-Twinning-Call for proposals “Strengthening the cyber security capacities of North Macedonia”*

**(a) Purpose of the grant(s)**

This call for proposals will aim at the implementation of *Output 1: Introduced operational tools for improving cyber-security and resilience and responding effectively to cyber-attacks, challenges and risks*

**(b) Type of applicants targeted**

The applicants must be EU Member State administrations or mandated bodies. The essential selection criterion is the operational capacity of the applicant. The essential award criteria are the technical expertise of the applicant and the relevance, methodology and sustainability of the proposed action. The maximum possible rate of EU financing may be up to 100% of the total cost of the action in accordance with Article 192 of the Financial Regulation if full funding is essential for the action to be carried out.

1. ***Grant-Twinning-Call for proposals “Improving performance of the police and law enforcement agencies”***

**(a) Purpose of the grant**

This call for proposals will aim at the implementation of *Output 2. Strengthened capabilities of the police and law enforcement agencies to combat and prevent crime, terrorism and radicalisation and manage security-related incidents, risks and crises.*

**(b) Type of applicants targeted**

The applicants must be EU Member State administrations or mandated bodies. The essential selection criterion is the operational capacity of the applicant. The essential award criteria are the technical expertise of the applicant and the relevance, methodology and sustainability of the proposed action. The maximum possible rate of EU financing may be up to 100% of the total cost of the action in accordance with Article 192 of the Financial Regulation if full funding is essential for the action to be carried out.

# Direct Management (Procurement)

Procurement will be used for achieving the activity related to the ICT hardware and software for the implementation of outcome 1*.*

# Scope of geographical eligibility for procurement and grants

The geographical eligibility in terms of place of establishment for participating in procurement and grant award procedures and in terms of origin of supplies purchased as established in the basic act and set out in the relevant contractual documents shall apply, subject to the following provisions.

The Commission’s authorising officer responsible may extend the geographical eligibility on the basis of urgency or of unavailability of services in the markets of the countries or territories concerned, or in other duly substantiated cases where application of the eligibility rules would make the realisation of this action impossible or exceedingly difficult (Article 28(10) NDICI-Global Europe Regulation).

# Indicative Budget

|  |  |  |
| --- | --- | --- |
| **Indicative Budget components** | **EU contribution**  **(amount in EUR)** | **Indicative third-party contribution, in currency identified** |
| **Output 1.1:**  Strengthened state response to security threats and risks, posed by cyber-crime, organised crime, terrorism, radicalisation and violent extremism. | **3 000 000** | **200 000** |
| Grants (direct management) – cf. section 4.3.1 | 2 000 000 |  |
| Procurement (direct management) – cf. section 4.3.2 | 1 000 000 | 200 000 |
|  |  |  |
| **Output 1.2:** Strengthened capabilities of the police and law enforcement agencies to combat and prevent crime, terrorism and radicalisation and manage security-related incidents, risks and crises | **2 000 000** |  |
| **Grants (direct management) – cf. section 4.3.1** | 2 000 000 |  |
|  |  |  |
| **Grants** – total envelope under section 4.3.1 | 4 000 000 |  |
| **Procurement** – total envelope under section 4.3.2 | 1 000 000 | 200 000 |
| **Evaluation** – cf. section 5.2 | Will be covered by another Decision | N.A. |
| **Audit/Expenditure verification** – cf. section 5.3 | Will be covered by another Decision | N.A. |
| **Strategic Communication and Public Diplomacy** – cf. section 6 | Will be covered by another Decision | N.A. |
| **Contingencies**[[29]](#footnote-30) | **0** | N.A. |
| **Totals** | **5 000 000** | **200 000** |

# Organisational Set-up and Responsibilities

# The Delegation of the European Union (EUD) to North Macedonia is in charge of the implementation of the Action, and will collaborate with the NIPAC Office within the Secretariat for European Affairs (SEA), the line ministries involved and all stakeholders and implementing partners.

# At the policy level, the implementing partners will be accountable to the relevant Sector Working Group (Home Affairs), as well as the IPA Monitoring Committee.

# At the contract level, the implementation arrangements will be discussed through the project Steering Committees having advisory functions and composed of EUD, the relevant national authorities and all relevant implementing partners.

As part of its prerogative of budget implementation and to safeguard the financial interests of the Union, the Commission may participate in the above governance structures set up for governing the implementation of the action.

# PERFORMANCE MEASUREMENT

# Monitoring and Reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process, and part of the implementing partner’s responsibilities. To this aim, the implementing partner shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its Outputs and contribution to the achievement of its Outcomes, and if possible at the time of reporting, contribution to the achievement of its Impacts, as measured by corresponding indicators, using as reference the logframe matrix (for project modality) and [the partner’s strategy, policy or reform action plan list (for budget support).

The Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

Arrangements for monitoring and reporting, including roles and responsibilities for data collection, analysis and monitoring: the progress in the implementation of the Action will be monitored at the sector level through the established 2020 Performance Assessment Framework (PAF), which includes outcome and impact indicators, targets and baseline data. PAF has been established as a web-based application (backed up by a government decision on responsibilities and deadlines), allowing regular electronic data input, processing, and analytics. The PAF data will be used in the Sector Working Group on Home Affairs, which is also the inclusive platform for all stakeholders to monitor the implementation of the sector priorities.

# Evaluation

Having regard to the importance of the action, a final evaluation will be carried out for this Action or its components via independent consultants. It will be carried out for accountability and learning purposes at various levels (including for policy revision).

The Commission shall form a Reference Group (RG) composed by representatives from the main stakeholders at both EU and national (representatives from the government, from civil society organisations (private sector, NGOs, etc.), etc.) levels. If deemed necessary, other donors will be invited to join. The Commission shall inform the implementing partner at least 2 months in advance of the dates envisaged for the evaluation exercise and missions. The implementing partner shall collaborate efficiently and effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities].

The evaluation reports shall be shared with the partner country and other key stakeholders following the best practice of evaluation dissemination. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner country, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project.

# Audit and Verifications

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audit or verification assignments for one or several contracts or agreements.

# STRATEGIC COMMUNICATION AND PUBLIC DIPLOMACY

All entities implementing EU-funded external actions have the contractual obligation to inform the relevant audiences of the Union’s support for their work by displaying the EU emblem and a short funding statement as appropriate on all communication materials related to the actions concerned. To that end they must comply with the instructions given in the 2022 guidance document [*Communicating and raising EU visibility: Guidance for external actions*](https://international-partnerships.ec.europa.eu/knowledge-hub/communicating-and-raising-eu-visibility-guidance-external-actions_en) (or any successor document).

This obligation will apply equally, regardless of whether the actions concerned are implemented by the Commission, the partner country, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU Member States. In each case, a reference to the relevant contractual obligations must be included in the respective financing agreement, procurement and grant contracts, and contribution agreements.

Any actions related to communication and visibility will be coordinated with the strategic communication actions of the EU Delegations, to ensure coherence of narrative and message, as well as horizontal strategic communication. Implementing partners shall keep the Commission and the EU Delegation/Office fully informed of the planning and implementation of specific visibility and communication activities before the implementation. Implementing partners will ensure adequate visibility of EU financing and will report on visibility and communication actions as well as the results of the overall action to the relevant monitoring committees

For the purpose of enhancing the visibility of the EU and its contribution to this action, the Commission may sign or enter into joint declarations or statements, as part of its prerogative of budget implementation and to safeguard the financial interests of the Union

# SUSTAINABILITY

Full ownership of the reform process in the home affair sector and the fight against organised crime and terrorism by the institutions of North Macedonia, based on coherent strategies that align with the EU acquis and good international practices, is a cornerstone of its sustainability. The Action’s sustainability is ensured through the improved capacities of the national authorities to fight cybercrime, organised crime and terrorism. This involves an upgrade of the operational and legal framework for fighting crime through establishing and/or amending procedures, rules and strategic documents, which will define in a mid-term anti-crime activities and routine in the country. In addition, training of officers and staff engaged in fighting crime will allow improving of the working methods in line with the EU standards allowing law enforcement bodies to participate in joint operations with EU and US and others peers, thus contributing to the country’s integration into the international anti-crime systems.

**Appendix 1: IDENTIFICATION OF THE PRIMARY INTERVENTION LEVEL FOR REPORTING IN OPSYS**

A Primary intervention[[30]](#footnote-31) (project/programme) is a coherent set of results structured in a logical framework aiming at delivering development change or progress. Identifying the level of the primary intervention will allow for:

* Differentiating these Actions or Contracts from those that do not produce direct reportable development results, defined as support entities (i.e. audits, evaluations);
* Articulating Actions and/or Contracts according to an expected common chain of results and therefore allowing them to ensure a more efficient and aggregated monitoring and reporting of performance;
* Having a complete and exhaustive mapping of all results-bearing Actions and Contracts.

The present Action identifies as

|  |  |  |
| --- | --- | --- |
| **Action level** (i.e. Budget support, Blending) | | |
|  | Single action | Present action: all contracts in the present action |
| **Group of actions level** (i.e: i) top-up cases, ii) second, third, etc. phases of a programme) | | |
|  | Group of actions | N/A |
| **Contract level** (i.e. Grants, Contribution Agreements, any case in which foreseen individual legal commitments identified in the budget will have different log frames, even if part of the same Action Document) | | |
|  | Single Contract 1 | N/A |
| **Group of contracts level** (i.e: i) series of programme estimates, ii) cases in which an Action Document foresees many foreseen individual legal commitments (for instance four contracts and one of them being a Technical Assistance) and two of them, a technical assistance contract and a contribution agreement, aim at the same objectives and complement each other, iii) follow up contracts that share the same log frame of the original contract) | | |
|  | Group of contracts | N/A |

1. This section is to be completed by the EU Office/Delegation. [↑](#footnote-ref-2)
2. Depending on the availability of OPSYS at the time of encoding, a provisional CRIS number may need to be provided. [↑](#footnote-ref-3)
3. Please specify if this action is going to be part of the Team Europe approach. [↑](#footnote-ref-4)
4. Indicate the lead window and thematic priority as identified in the relevant programming document. Please indicate for each thematic priority the approximate share (%) of the window budget it represents. [↑](#footnote-ref-5)
5. Development Assistance Committee (DAC) sectors (codes and descriptions) are indicated in the first and fourth columns of the tab ‘purpose codes’ in the following document: [DAC and CRS code lists - OECD](https://www.oecd.org/development/financing-sustainable-development/development-finance-standards/dacandcrscodelists.htm) [↑](#footnote-ref-6)
6. For guidance, see [Development finance standards - OECD](https://www.oecd.org/development/financing-sustainable-development/development-finance-standards/) (Go to “Data collection and resources for reporters”, select Addendum 2, annexes 18 (policy) and 19 (Rio) of the reporting directive. If an action is marked in the DAC form as contributing to one of the general policy objectives or to RIO principles as a principal objective or a significant objective, then this should be reflected in the logframe matrix (in the results chain and indicators). [↑](#footnote-ref-7)
7. Please check the [Handbook on the OECD-DAC Nutrition Policy Marker](https://scalingupnutrition.org/wp-content/uploads/2020/12/OECD_PolicyMarkerNutrition.pdf). [↑](#footnote-ref-8)
8. These markers have a different scope/rationale than the DAC codes. They are drawn from the level of budget allocation and emphasise the action in terms of main objective(s) selected. The definition of objectives and outputs in the description of the action should be in line with this section. [↑](#footnote-ref-9)
9. When a marker is Significant or Principal Objective, please indicate the relevant tags by selecting “YES” or “NO”. [↑](#footnote-ref-10)
10. Please address the digitalisation marker in line with the note ARES(2019)7611708, which provides internal guidelines on the criteria to be used to assess the degree of relevance of the marker for the action (not targeted, significant or main objective). [↑](#footnote-ref-11)
11. When a marker is “Significant Objective“ or “Principal Objective”, please indicate the relevant tags by selecting “YES” or “NO”. [↑](#footnote-ref-12)
12. Please address the migration marker in line with the note Ares(2021)6077013. [↑](#footnote-ref-13)
13. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [↑](#footnote-ref-14)
14. https://ncsi.ega.ee/country/mk/?fbclid=IwAR0- [↑](#footnote-ref-15)
15. https://www.consilium.europa.eu/media/36546/joint-action-plan-on-ct-for-wb.pdf [↑](#footnote-ref-16)
16. Principal objective / significant objective/ not targeted. [↑](#footnote-ref-17)
17. <https://info.worldbank.org/governance/wgi/Home/Reports> [↑](#footnote-ref-18)
18. <https://info.worldbank.org/governance/wgi/Home/Reports> [↑](#footnote-ref-19)
19. <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=crim_off_cat&lang=en> [↑](#footnote-ref-20)
20. PPO Annual Report [↑](#footnote-ref-21)
21. <https://europa.eu/eurobarometer/surveys/browse/all/series/4961> [↑](#footnote-ref-22)
22. Financial Police-Criminal Intelligence Unit. [↑](#footnote-ref-23)
23. Numerator: Number of people under financial investigation within DSOSC 57 (43 individuals and 14 legal entities) // Denominator: Total number of persons under investigation within DSOSC [↑](#footnote-ref-24)
24. Financial Police [↑](#footnote-ref-25)
25. Report of the Agency for confiscation of Assets [↑](#footnote-ref-26)
26. <https://ec.europa.eu/neighbourhood-enlargement/system/files/2021-10/North-Macedonia-Report-2021.pdf> [↑](#footnote-ref-27)
27. This section is to be completed by the EU Office/Delegation. [↑](#footnote-ref-28)
28. [EU Sanctions Map](https://www.sanctionsmap.eu/#/main). Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails. [↑](#footnote-ref-29)
29. Consider that contracts where no financing agreement is concluded, contingencies have to be covered by individual and legal commitments by 31 December of N+1. [↑](#footnote-ref-30)
30. For the purpose of consistency between terms in OPSYS, DG INTPA, DG NEAR and FPI have harmonised 5 key terms, including ‘Action’ and ‘Intervention’ where an ‘Action’ is the content (or part of the content) of a Commission financing Decision and ‘Intervention’ is a coherent set of activities and results which constitutes an effective level for the operational follow-up by the EC of its operations on the ground. See more on the [concept of intervention](https://webgate.ec.europa.eu/fpfis/wikis/display/PCM/Concept+of+intervention) *[to access the link an EU Login is needed]*. [↑](#footnote-ref-31)