Twinning Fiche

Project title: "Enhancing Performance of Police, Law Enforcement, and Cybersecurity"

Beneficiary administration: Ministry of Interior of Republic of North Macedonia

Twinning Reference: MK 24 IPA JH 01 26

Publication notice reference: **EuropeAid/187202/DD/ACT/MK**

EU funded project

TWINNING TOOL

Acronyms and Abbreviations

IPA	Instrument for Pre-Accession Assistance
BC	Beneficiary Country (the country receiving assistance)
EC	European Commission
EU	European Union
IPA III	Instrument for Pre-Accession Assistance (Third Phase)
MS	Member State (in the context of the Twinning project)
MoI	Ministry of Interior of the Republic of North Macedonia
SAA	Stabilization and Association Agreement
JHA	Justice and Home Affairs
EC Report	European Commission Report
NATO	North Atlantic Treaty Organization
SOCTA	Serious and Organised Crime Threat Assessment
FTFs	Foreign Terrorist Fighters
CERT	Computer Emergency Response Team
ICT	Information and Communication Technologies
JAD	Joint Action Days
OSCE	Organization for Security and Co-operation in Europe
UNDP	United Nations Development Programme
SIENA	Secure Information Exchange Network Application
ICSE	International Child Sexual Exploitation database
EMPACT	European Multidisciplinary Platform Against Criminal Threats
CSIRT	Computer Security Incident Response Team
UNODC	United Nations Office on Drugs and Crime
LEAs	Law Enforcement Agencies
ENISA	European Union Agency for Cybersecurity
EUD	European Union Delegation

1. Basic Information

1.1 Programme: EU for Rights and Security, Annual action plan in favour of North Macedonia for 2024; IPA III-ENEST/2024/045-609 (EC); OPSYS business reference: ACT-62397; ABAC Commitment level 1 number: JAD.1354913
1.2 Twinning Sector: Justice and Home Affairs
1.3 EU funded budget: 4.000.000,00 EUR
1.4 Sustainable Development Goals (SDGs): SDG 16 Peace, Justice and Strong Institutions

2. Objectives

2.1 Overall Objective(s):

The overall objective of this project is to improve the security architecture of North Macedonia.

2.2 Specific objective:

The specific objective is to significantly strengthen the capacity of national institutions to detect, investigate, prosecute, and prevent security threats and risks related to cybercrime, organized crime, terrorism, radicalization, and violent extremism.

2.3 The elements targeted in strategic documents i.e. National Development Plan/Cooperation agreement/Association Agreement/Sector reform strategy and related Action Plans

Strategic Plan of the Ministry of Interior of the Republic of North Macedonia (2024-2026)

The Ministry of Interior's Strategic Plan (2024–2026) outlines measures grouped into programs and sub-programs to strengthen the rule of law, improve efficiency, and ensure transparency in combating organized crime, corruption, illegal migration, terrorism, and cyber threats. These priorities align with the Government's strategic goals for 2024–2028.

National Strategy for combating terrorism (2023-2027) and National Strategy for preventing violent extremism (2023-2027)
The National Strategies for Countering Terrorism and Preventing Violent Extremism (2023–2027), prepared with broad stakeholder involvement, focus on preventing radicalization, strengthening institutional capacities, and ensuring respect for human rights, in line with UN and EU standards.

Cyber Security Strategy (2025-2028)
The Cyber Security Strategy (2025–2028) aims to build a secure and resilient digital environment through coordinated national responses, risk-based approaches, and capacity development, following ITU and ENISA guidelines.

Law on the Security of Network and Information Systems (NIS2)

The Law on the Security of Network and Information Systems represents a key legal instrument for regulating cybersecurity. The Law establishes the institutional framework, defines risk management measures, regulates the incident reporting system, and provides for the establishment of Computer Security Incident Response Teams (CSIRTs). It is aligned with the European Union NIS2 Directive and serves as a foundation for strengthening cyber resilience, in particular within critical sectors and public administration.

With the adoption of the Law on the Security of Network and Information Systems, the Ministry of Digital Transformation is designated as the competent authority for the security of network and information systems. In this role, the Ministry proposes strategies, action plans, and regulations in the field of cybersecurity, prepares annual work plans and reports, and develops plans for responding to cyber threats and incidents in coordination with MKD-CIRT and other relevant authorities. It also develops guidelines, protocols, and technical rules for the assessment and enhancement of security within the public sector.

The Ministry is responsible for handling cybersecurity incidents, issuing warnings and information on risks, maintaining records and registers of incidents, critical sectors, and entities, and exchanging information with national and international partners. Furthermore, it performs the functions of the governmental CSIRT (MKD-GOV-CSIRT) and the Single Point of Contact (SPOC), while providing support to mechanisms for information sharing and cooperation.

In addition, the Ministry promotes the use of open tools and standards, participates in the drafting of laws, policies, and strategic documents, and carries out supervision over essential and important entities in accordance with the Law. It organizes training programmes, awareness-raising campaigns, and other capacity-building activities, administers the national cybersecurity portal, and performs other responsibilities as prescribed by law.

Council Decision 2008/212/EC of 18 February 2008 on the principles, priorities and conditions contained in the Accession Partnership with the Republic of North Macedonia

The Decision sets priorities and conditions for North Macedonia's EU accession, emphasizing obligations under the Stabilization and Association Agreement and sectoral reforms. It highlights the importance of technical assistance and institutional capacity building to meet EU membership requirements.

Stabilization and Association Agreement (SAA)

The SAA supports North Macedonia's economic and international cooperation by aligning national legislation with EU law, fostering integration into the European market, and strengthening governance.

European Commission Report

The EC notes moderate progress in fighting organized crime and terrorism, but limited alignment with EU acquis. Key challenges include weak operational capacity, insufficient resources, and gaps in legislation on cybercrime, child protection, and critical infrastructure. Cooperation with Europol is positive, but reforms remain necessary.

Regulation (EU) 2021/784

This regulation requires online platforms to swiftly remove terrorist content, often within one hour of notification, to prevent radicalization and protect public security. It applies to all providers serving EU users.

National Strategy for building resilience and confronting hybrid threats (2021-2025)

The strategy strengthens national resilience against hybrid threats by raising awareness, defining responsibilities, mobilizing resources, and engaging society to detect, respond to, and recover from crises.

Economic and Investment Plan for the Western Balkans

The EU plan enhances regional security and development by supporting judicial cooperation, law enforcement, and cybercrime prevention. It also promotes digital transformation and resilience against evolving threats.

Growth Plan and Reform Agenda

The Growth Plan provides €6 billion to accelerate EU integration. North Macedonia's Reform Agenda focuses on governance, digital transition, human capital, private sector growth, and rule of law, with EU approval unlocking funds for reforms.

3. Description

3.1 Background and justification:

Organised crime and terrorism

North Macedonia remains vulnerable to organised crime due to its geographic position as a transit hub. Key challenges include drug trafficking, migrant smuggling and trafficking in human beings, arms trade, and money laundering. Despite progress in aligning with EU standards, enforcement gaps, corruption, and limited interagency cooperation persist. The European Commission highlights the need for stronger operational coordination, financial investigations, and asset confiscation.

Terrorism and radicalisation also pose risks, particularly linked to foreign terrorist fighters and online propaganda. National strategies for countering violent extremism and terrorism are in place, but further improvements in detection, prevention, and coordination with EU and regional partners are required.

Cybercrime and cyber security

Growing reliance on digital services has increased exposure to cyber incidents such as ransomware, data breaches, and online fraud. While North Macedonia has adopted legislation and established a national CERT, challenges remain in cyber forensics, institutional

coordination, and technical expertise. Strengthening national capacities and aligning with EU cybersecurity standards are essential to ensure resilience and public trust.

3.2 Ongoing reforms:

The Project is in line with the EU Strategy for Western Balkans, with main aim being to support the country in adopting and implementing the institutional, legal, administrative reforms required to comply with Union values and to progressively align to Union rules, standards, policies and practices with a view to Union membership, thereby contributing to country's stability, security and prosperity.

Furthermore, the completion of Project's results will contribute towards the implementation of the Stabilization and Association Agreement (SSA) regarding the statements stipulated in article 78 concerning trafficking in human beings; illegal economic activities, preventing and combating crime and other illegal activities, including corruption and illegal economic activities, etc.

The Project is contributing to the objectives of United Nation's 2030 Agenda for Sustainable Development; more specifically, the action contributes to SDG 16 Peace, Justice and Strong Institutions. More specifically, North Macedonia is implementing SDG 16 within its strategic framework through the specific objectives and measures related to the reduction of illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organised crime, strengthen relevant national institutions, including through international cooperation to prevent violence and combat terrorism and crime, etc. The monitored indicators are regularly updated by the National Statistical Institute.

The project will contribute for the Public Administration Reform efforts of the country and it is in line with the PAR Strategy 2023-2030 supporting the establishment of professional and competent administrative officers in the field of protection of the environment and the cultural heritage of the country; effective application of modern information technologies and in overall high-quality services delivered to the citizens and businesses.

The Project is also in line with the Joint Action Plan on Preventing and Countering of Terrorism and Violent Extremism for the Western Balkans, which aims to increase alignment to EU legislation, bolsters operational cooperation with EU agencies and promotes regional cooperation in countering terrorism and preventing violent extremism. The JAP is also focused on stepping up capacities on Prevention of violent extremism, dealing with emerging threats such as ethno-nationalist violent extremism and, online radicalization; Counter terrorism Financing and critical infrastructure resilience. This initiative aligns with the EU's Strategy for the Western Balkans and the Sofia Declaration of May 2018, emphasizing enhanced security collaboration among the region's countries.

In October 2025, North Macedonia further committed to this framework by signing the new Joint Action Plan on Preventing and Countering of Terrorism and Violent Extremism for the Western Balkans, which introduced new actions and more ambitious targets, reflecting the evolving nature of security threats and the need for adaptive responses.

Internationally, North Macedonia collaborates with various partners, including the European Union, the United States, and regional organizations like the Organization for Security and Co-

operation in Europe (OSCE) and the United Nations Office on Drugs and Crime (UNODC). This cooperation encompasses joint training programs, information sharing, and participation in regional projects aimed at combating terrorism and its financing.

3.3 Linked activities:

"Combatting sexual and gender-based violence in the Digital sphere"- a project implemented by UNDP

- Combating online sexual and gender-based violence through strengthening the capacities of the Ministry of Interior is the main goal of the project which will be implemented by the United Nations Development Programme (UNDP) in collaboration with the MOI. As part of the project the following activities have been implemented:
- Online training organized by UNDP, held from 7–9 August 2023, focused on enhancing the capacities of legal and judicial authorities to address gender-based violence in the digital environment. This was followed by a study visit to the Republic of Korea (21–29 June 2024), aimed at benchmarking international best practices.
- From 29-31 October 2024 - held specialized training on online gender-based violence for police officers, public prosecutors and service providers;

"EU Support for rule of law"- national IPA 2020 project;

- The objective of the project is to strengthen the rule of law in North Macedonia. The project is designed to support vital institutions operating in the fields of justice, law enforcement, anti-corruption efforts, and the promotion and protection of fundamental and human rights. It aims to enhance their capacities, effectiveness, and impact through a multifaceted approach.

"Western Balkans Partnership against Crime and Terrorism project-phase 2" (2024-2028) – regional IPA project implemented by CEPOL, also supported by Europol

- The second phase of the Western Balkans Partnership against Crime and Terrorism project (WB PaCT) aims to further enhance the operational and strategic capacities of authorities in the Western Balkans to fight organised crime and terrorism.

"Law Enforcement Records, Data and Case Management System" (LERMS) – national IPA 2021 project

- The aim of this project is establishment of an IT Tool: Law Enforcement Record Management System (LERMS) at the Law Enforcement Agencies (LEAs) of the Republic of North Macedonia that will ensure record management and tracking of records of law enforcement operations and investigations in suppressing organized crime, corruption, terrorism and other types of crime; providing analytical functionalities for generating structured data and supplementing the data exchange by different LEA with reliable data.

"CyberSEE - Project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye"

- The overall objective of CyberSEE is to strengthen the rule of law, security and regional co-operation in the South-East-Europe and Türkiye through a more effective response to the challenges of cybercrime and electronic evidence. Under this overall objective, the Project implements activities in the region with the specific objective to reach strengthened and more effective criminal justice response of Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Türkiye and Kosovo to cybercrime and electronic evidence, in line with the provisions of the Budapest Convention on Cybercrime, its Second Protocol and European Union objectives.

IISG (Integrative Internal Security Governance) process

- The IISG (Integrative Internal Security Governance) process has been initiated as part of the EU's decisive action to improve cooperation with the Western Balkans region on security issues. The concept enables a coordinated, aligned, and sustainable effort in the major fields of internal security governance reform on part of the EU and all relevant international donors of external assistance. The objective of the IISG is to improve collective efficiency by mapping needs and coordinating responses concerning security threats in the Western Balkan region. For this purpose, the IISG is a coordination platform bringing together relevant international partners, Western Balkans partners, EU actors and EU Member States in the areas of counter-terrorism, organised crime and border security, in line with the EU perspective for the region.

"Strengthening the capacities of the penitentiary system in North Macedonia"

- Building upon the results achieved from the implementation of the first and the second phase of the "Horizontal Facility for the Western Balkans and Türkiye", a joint programme of the European Union and the Council of Europe, the Action "Strengthening the capacities of the penitentiary system in North Macedonia" assists the authorities in progressing further with the country's prison reform agenda and enhancing the protection of the human rights of prisoners and detained persons. It is implemented in close cooperation and partnership with the Ministry of Justice (Directorate for Execution of Sanctions), Ministry of Health, Ministry of Interior, the Public Prosecutor's Office and the Ombudsman's Office, as well as other national stakeholders, including prominent civil society organisations active in the area of protection and promotion of human rights.

"Improving the Resilience of Critical Entities and the Protection of Public Spaces and Cyberspace against Security Threats in the Western Balkans" (WB CEPS & Cyber)

- The EU-funded project "Improving the Resilience of Critical Entities and the Protection of Public Spaces and Cyberspace against Security Threats in the Western Balkans" (WB CEPS & Cyber) officially kicked off in May 2026. The project is focused on strengthening the resilience of critical entities, public spaces and cyberspace across the region by bringing together two complementary components — one centred on cyber capacity building, and the other on the legal and institutional frameworks for protection of critical infrastructure. The WB3C component focuses on people and practice. Over the next three years, it will deliver targeted training, mentoring and technical support in cybersecurity, cybercrime and cyber diplomacy — with a strong emphasis on applied skills, operational readiness, and cooperation between institutions. In parallel, the CEPS component, led by CIVIPOL in cooperation with the Ministries of Interior of France,

Italy, Croatia and Greece, works on strengthening legal alignment, institutional frameworks and regional coordination mechanisms for the protection of critical entities and public spaces.

"EU Support to Strengthen the Fight against Migrant Smuggling and Trafficking in Human Beings in the Western Balkans" (EU4FAST)

- The project aims to reinforce the rule of law in the Western Balkans by strengthening the capacities of the national and regional authorities for preventing and combatting migrant smuggling and trafficking in human beings. A tailored approach in line with the specific needs of the partners will be directed towards all relevant institutions and stakeholders to enhance capacities on an institutional and individual level to ensure efficient identification and protection to (potential) victims of trafficking in human beings as well as to refer them to relevant state and non-state support services.

"Strengthening Management Systems of Irregular Migration and Fight against Organised Crime in North Macedonia"

- This project is implemented by the International Organization for Migration (IOM) in close cooperation with key institutional stakeholders, primarily the Ministry of Interior, the Ministry of Social Policy, Demography and Youth, the Ministry of Health, and others relevant entities, with a focus on strengthening the country's capacity in border management, reducing cross-border crimes and addressing irregular migration in line with EU standards. Over the course of four years, the project will aim to strengthen the capacities of relevant national institutions in border management, surveillance, and combating organised crime in line with fundamental rights, while enhancing the protection of vulnerable migrants and supporting the sanctioning of smugglers.

"Strengthening anti-trafficking action in North Macedonia"

- The action "Strengthening Anti-Trafficking Action in North Macedonia", implemented within the joint programme of the European Union and the Council of Europe "Horizontal Facility for the Western Balkans and Türkiye" for the period January 2023–December 2026, aims to strengthen legislation, policies, and practices for effectively combating trafficking in human beings, protecting victims' rights, and addressing emerging challenges and trends; enhance the criminal justice response to trafficking through capacity building and research; and improve mechanisms and procedures enabling victims of trafficking to access legal remedies, sustainable support services, and compensation.

The envisaged Twinning Project will ensure close coordination with ongoing national and regional initiatives implemented by the EU, Council of Europe, UN agencies, CEPOL, Europol, IOM and other international partners in the areas of rule of law, organised crime, cybercrime, trafficking in human beings, migration management, and institutional capacity building. Particular attention will be paid to creating synergies with projects such as the UNDP project "Combatting Sexual and Gender-Based Violence in the Digital Sphere", the IPA-funded "EU Support for Rule of Law", the regional "Western Balkans Partnership against Crime and Terrorism" (WB PaCT 2), the "Law Enforcement Records, Data and Case Management System" (LERMS), CyberSEE, the IISG process, EU4FAST, and other ongoing initiatives supporting

border management, anti-trafficking measures, cyber resilience, and penitentiary reforms. Coordination mechanisms will include regular consultations with relevant institutions and donors, participation in existing coordination platforms, exchange of information and lessons learned, and alignment of activities with national strategies and EU priorities. The project will build upon existing results, complement already established capacities and systems, and avoid duplication through continuous stakeholder engagement and mapping of ongoing interventions, while promoting interoperability, institutional cooperation, and sustainable long-term impact.

3.4 List of applicable *Union acquis*/standards/norms:

- Chapter 24 of the EU Acquis on Justice, Freedom and Security
- Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online
- Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
- Council of the EU Conclusions on EU External Action on Counter-terrorism
- Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
- Council Framework Decision 2002/475/JHA on combating terrorism
- Directive 2012/29/EU recognizing that victims of terrorism
- Council Framework Decision 2004/757/JHA of 25 october 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking
- Regulation (EU) 2025/13 and with Directive (EU) 2016/681 on the collection, transfer and processing of Advance Passenger Information (API) and Passenger Name Records (PNR)
- Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended.
- Directive (EU) 2018/1673 on combatting money laundering by criminal law.
- Directive (EU) 2024/1260 on asset recovery and confiscation
- Framework Decision 2008/841/JHA on the fight against organised crime
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto assets.
- Directive EU/2022/2557 on the resilience of critical entities Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences
- Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity across the Union
- ENISA guidelines and standards for cyber resilience and CSIRT collaboration

3.5 Components and results per component

The project is consisting of 2 components:

Component 1: Strengthening the strategic and operational capacities of law enforcement agencies to prevent and combat organised crime and security threats in line with EU and international standards

Mandatory result 1: National strategic, operational and investigative capacities of law enforcement agencies strengthened to effectively prevent and combat organised crime, including migrant smuggling, trafficking in human beings, drug trafficking, firearms trafficking, and related security threats, in line with EU acquis and international standards.

Sub-result 1.1: Strategic and organisational framework strengthened

Expected sub-results:

1) National legal, institutional and organisational frameworks for combating organised crime are reviewed and recommendations prepared for alignment with EU acquis and international standards;
2) Strategic coordination and planning capacities for joint law enforcement action are strengthened;
3) Inter-agency cooperation and information exchange mechanisms are enhanced, including cooperation with law enforcement agencies (LEAs);
4) Institutional needs and capacity gaps are identified with recommendations for strengthening organisational structures, specialised units, and interoperability, including IT and data management capacities;
5) Proposals are developed to improve secure information exchange and interoperability with relevant national and international systems and databases.

Sub-result 1.2: Operational and investigative capacities strengthened

Expected sub-results:

1) Operational procedures and investigative practices are reviewed and improved in line with EU best practices;
2) Capacities in modern investigative methods and analytical approaches, including digital forensics, HUMINT, and financial investigations, are strengthened;
3) Training needs are identified and training curricula developed covering criminal intelligence, investigative techniques, evidence collection, and cyber-hybrid crime;
4) Targeted trainings are delivered to strengthen operational and analytical capacities of law enforcement officers;
5) Operational capacities are strengthened for the investigation and prosecution of organised crime, including trafficking in human beings, migrant smuggling, drug trafficking, and firearms trafficking, with a focus on victim-sensitive and cross-border cooperation approaches;
6) Methodological guidance is developed to support the distinction between trafficking in human beings and migrant smuggling in line with EU standards.

Sub-result 1.3: National and international cooperation strengthened

Expected sub-results:

1) Cooperation frameworks with EU Member States, EU agencies (including Europol, Eurojust, Frontex), FIUs, ARO platforms, and relevant international networks are strengthened;
2) Cooperation mechanisms between national law enforcement institutions and LEAs are enhanced, including secure and timely information exchange;
3) Operational coordination arrangements for cross-border investigations and joint actions are strengthened;
4) Joint operational exercises and coordination activities are implemented to enhance readiness and cooperation;
5) Good practices and lessons learned from national and international cooperation are integrated into institutional procedures and frameworks.

Component 2: Strengthening national cybersecurity resilience

Mandatory Result 2:
National cybersecurity resilience and cybercrime response capacities are enhanced through improved operational procedures, institutional coordination, information sharing, technical capabilities, and awareness, in line with EU cybersecurity standards and best practices

Sub-result 2.1: Operational capacities for cyber threat prevention, detection and response strengthened

Expected sub-results:

1) Needs assessment conducted and recommendations prepared to strengthen cybersecurity governance, operational coordination, and technical infrastructure;
2) Operational procedures, escalation protocols, and cyber incident response arrangements developed and improved in line with EU best practices;
3) Cooperation mechanisms between CSIRTs, law enforcement authorities, prosecutors, and relevant stakeholders strengthened for coordinated cyber incident response and cybercrime investigation;
4) Capacities strengthened for cybercrime investigation, digital forensics, handling of electronic evidence, and incident attribution;
5) Targeted trainings and operational exercises delivered to enhance readiness and response to cyber threats;
6) Joint simulation and operational exercises conducted to test inter-agency coordination and response capabilities.

Sub-result 2.2: National, regional and international cyber cooperation strengthened

Expected sub-results:

1) National Single Point of Contact (SPOC) for international cyber cooperation established and operationalised;
2) Information-sharing mechanisms between national cybersecurity institutions and law enforcement agencies (LEAs) strengthened;

3) Cooperation with EU and international cyber networks and organisations further developed and enhanced;
4) Secure communication channels and procedures for cyber threat intelligence and incident information exchange between cybersecurity institutions and LEAs established and operationalised;
5) Joint coordination mechanisms for cross-border cyber incident response strengthened;
6) Staff capacities enhanced for effective international cooperation and information exchange during cyber incidents.

Sub-result 2.3: Cybersecurity awareness, training and capacity building strengthened

Expected sub-results:

1) Training needs assessment conducted and training curricula developed for relevant institutions;
2) Training programmes delivered on cybercrime investigation, digital evidence handling, and cyber incident response;
3) Awareness-raising activities implemented on cyber hygiene, cyber threats, and protection of critical infrastructure;
4) Practical exercises, workshops, and simulation activities conducted involving relevant stakeholders;
5) Operational guidance and good practices aligned with EU cybersecurity standards developed and applied.

Sub-result 2.4: National cyber risk assessment and preparedness strengthened

Expected sub-results:

1) National cyber risk assessment conducted in line with EU methodologies, with the involvement of law enforcement agencies (LEAs) in the threat assessment process;
2) Institutional capacities strengthened to integrate risk assessment findings into strategic planning, prioritisation, and decision-making processes;
3) National coordination and response arrangements for major cyber incidents developed, tested, and aligned with relevant national and EU frameworks;
4) Public awareness initiatives and scenario-based exercises implemented to strengthen cybersecurity preparedness and resilience.

3.6 Means/input from the EU Member State Partner Administration(s)*:

The project will be implemented between the final beneficiary country and EU Member State(s). The implementation of the project requires one Project Leader (PL) with responsibility for the overall coordination of project activities and one Resident Twinning Adviser (RTA) to manage implementation of project activities, Component Leaders (CL) and pool of short-term experts within the limits of the budget. It is essential that the team has sufficiently broad expertise to cover all the areas included in the project description.

Proposals submitted by Member State shall be concise and focused on the strategy and methodology and an indicative timetable underpinning this, the administrative model suggested,

the quality of the expertise to be mobilised and clearly show the administrative structure and capacity of the Member State entity/ies. Proposals shall be detailed enough to respond adequately to the Twinning Fiche, but are not expected to contain a fully elaborated project. They shall contain enough detail about the strategy and methodology and indicate the sequencing and mention key activities during the implementation of the project to ensure the achievement of overall and specific objectives and mandatory results/outputs.

The interested Member State(s) shall include in their proposal the CVs of the designated PL, Resident Twinning Advisor, as well as the CVs of the designated component Leaders-CLs.
The set of proposed activities will be further developed with the Twinning partners when drafting the initial work plan and successive rolling work plan every three months, keeping in mind that the final list of activities will be decided in cooperation with the Twinning partner.
The components are closely interlinked and need to be sequenced accordingly.

3.6.1 Profile and tasks of the PL:

Qualifications and skills:

- University degree or equivalent professional experience of 8 years;
- At least 3 years of relevant experience in the field;
- Fluency in written and spoken English;
- Prior experience in implementation of international and/or EU funded projects in the relevant area will be considered as an asset;

Tasks of the Project Leader:

- Conceive, supervise and coordinate the overall Twinning project;
- Coordinate and monitor the overall implementation of the project including coordination and direction of the MS Twinning partner;
- Coordinate MS experts' work and availability;
- Permanent contacts with the main counterpart in the BC;
- Ensure the backstopping functions and financial management;
- Guarantee from the MS administrative side, the successful implementation of the Project's Work Plan; participate in meetings of the Project Steering Committee with the BC PL;

3.6.2 Profile and tasks of the RTA:

One Resident Twinning Advisor (RTA) will be appointed and he/she will be located in the premises of the Ministry of Interior The secondment of the RTA will last for 48 months, during which he/she will be responsible for the direct implementation of the project under the overall supervision of the MS Project Leader.

Qualifications and skills:

- University Degree preferably in the relevant field of education in the project focus or equivalent professional experience of 8 years;
- At least 3 years of specific experience in MS administration in the relevant field;

- Experience in project implementation and/or coordination in international and/or EU funded project will be considered as an asset;
- Fluency in written and spoken English;

Tasks of the Resident Twinning Adviser

- Drafting and initial work plan in close cooperation with the relevant actors;
- Coordinate of all project activities and experts' inputs in the country;
- Ensure timely and correct implementation of the activities as outlined in the initial and subsequent work plans; keeps the Beneficiary PL informed about the implementation and reports regularly to the Member State PL;
- Updates the work plan to be transmitted to the Project Steering Committee under the authority of the Member State PL;
- Providing advice and assistance to the representatives of the Beneficiary administration;
- Monitoring and evaluating the needs and priorities in the respective sector, project risks, progress against the project budget, benchmarks, and outputs, and taking any necessary remedial actions if needed;
- Coordination of the EU MS experts' work and availability;
- Preparation of the materials and documentation for regular monitoring and reporting;
- Take corrective actions, if necessary, inside the terms of the signed contract.

RTA Assistant: The RTA will be provided with a full-time RTA assistant acting as an assistant for technical and organizational support. The assistant will be contracted according to Twinning rules and paid from the Twinning budget. The assistant will be selected through an open call. The role of RTA Assistant is to support the RTA in the project management. In addition, the assistant will be responsible for organization of meetings, seminars etc. and their logistics, as well as interpretation and translation.

Full time translator/interpreter: A full-time translator / interpreter will be selected through an open call and will be contracted according to the Twinning rules and paid from the Twinning budget. The full-time translator / interpreter will be involved in all necessary project activities (training sessions, translation of project documents/reports and materials, organizational activities, etc.). The role of the translator/ interpreter will be to provide translation and editing as well as interpretation services to the Twinning project in general.

3.6.3 Profile and tasks of Component Leaders*:*

Component Leader 1:

- University degree in the relevant field of education or equivalent professional experience of 8 years;
- At least 3 years of specific of relevant experience in the field of project focus
- Experience in project implementation and/or coordination in international and/or EU funded project will be considered as an asset;
- Fluency in written and spoken English;

Tasks:

- To supervise and coordinate the overall preparation of the activities under the component 1 in close cooperation with the RTA;

Component Leader 2:

- University degree in the relevant field of education or equivalent professional experience of 8 years;
- At least 3 years of specific of relevant experience in the field of project focus
- Experience in project implementation and/or coordination in international and/or EU funded project will be considered as an asset;
- Fluency in written and spoken English;

Tasks:

- To supervise and coordinate the overall preparation of the activities under the component 2 in close cooperation with the RTA.

3.6.4 Profile and tasks of other short-term experts*:*

Short Term Experts shall comply with the following minimum requirements:

- University degree preferably in the area relevant for the implementation of the project or equivalent professional experience of 8 years;
- At least 3 years of working experience in the relevant field
- Fluency in written and spoken English;
- Good skills in reporting and communication;

Tasks:

- Delivering expertise under the overall responsibility of the Member State PL and the coordination and supervision of the RTA;
- Delivering support to the Beneficiary administration through specific activities in the Beneficiary country, including workshops, seminars, training sessions, meetings with officials of the Beneficiary administration, joint drafting sessions, etc.;
- Preparation and reporting work, before and after missions to the Beneficiary country;
- Address cross-cutting issues;

4. Budget

The project will be implemented through a Twinning Contract estimated at maximum 4,000,000 EUR.

Twinning Contract	**Total (EUR)**	**IPA Community contribution**		**National Public contribution**	
		EUR	**%**	**EUR**	**%**
	4 000 000	**4 000 000**	**100**	**/**	**/**

5. Implementation Arrangements

5.1 Implementing Agency responsible for tendering, contracting and accounting (AO/CFCU/PAO/European Union Delegation/Office):

Mr. Steffen Hudolin
Head of Cooperation
European Union Delegation
St. Cyril and Methodius 52b,
1000 Skopje

Ms. Danica Stoshevska
Programme Manager
European Union Delegation
St. Cyril and Methodius 52b,
1000 Skopje

5.2 Institutional framework

The main beneficiary of this Twinning project will be The Ministry of Interior, in particular The Department for Suppression of Organized and Serious Crime (DSOSC) and the Sector for Computer crime within the Public Security Bureau.

5.3 Counterparts in the Beneficiary administration:

The PL and RTA counterparts will be staff of the Beneficiary administration and will be actively involved in the management and coordination of the project.

5.3.1 Contact person:

Mr. Stojan Ilijevski
Head of the Sector for IPA and community programmes, Department for EU and international cooperation
Coordinator
Ministry of Interior
St. Dimce Mircev N.9, 1000, Skopje

5.3.2 PL counterpart

Mr. Dejan Nikolovski
Head of Criminal Intelligence and Analysis Sector, Department for suppression of organised and serious crime, Bureau for Public Security
Ministry of Interior
St. Dimce Mircev N.9, 1000, Skopje

5.3.3 RTA counterpart
Mr. Dragan Cvetanovski
Chief Inspector in the Sector for Computer crime, Bureau for Public Security
Ministry of Interior
St. Dimce Mircev N.9, 1000, Skopje

Component Leader for Component 1
Mr. Vlatko Vakanski
Head of Sector for Combating Terrorism, Violent Extremism and Radicalism, Department for Suppression of Organized and Serious Crime, Bureau for Public Security
Ministry of Interior
St. Dimce Mircev N.9, 1000, Skopje

Component Leader for Component 2

Mr. Marijan Dimovski
Head of Sector for Computer Crime, Bureau for Public Security
Ministry of Interior
St. Dimce Mircev N.9, 1000, Skopje

6. Duration of the project

The implementation period of the Action will last **48 months**. The execution period of the contract shall enter into force upon the date of notification by the Contracting Authority of the contract signed by all parties, whereas it shall end 3 months after the implementation of the Action.

7. Management and reporting[1]

7.1 Language

The official language of the project is the one used as contract language under the instrument (English). All formal communications regarding the project, including interim and final reports, shall be produced in the language of the contract.

7.2 Project Steering Committee

A project steering committee (PSC) shall oversee the implementation of the project. The main duties of the PSC include verification of the progress and achievements via-à-vis the mandatory results/outputs chain (from mandatory results/outputs per component to impact), ensuring good coordination among the actors, finalising the interim reports and discuss the updated work plan. Other details concerning the establishment and functioning of the PSC are described in the Twinning Manual.

7.3 Reporting

All reports shall have a narrative section and a financial section. They shall include as a minimum the information detailed in section 5.5.2 (interim reports) and 5.5.3 (final report) of the Twinning Manual. Reports need to go beyond activities and inputs. Two types of reports are foreseen in the framework of Twining: interim quarterly reports and final report. An interim quarterly report shall be presented for discussion at each meeting of the PSC. The narrative part shall primarily take stock of the progress and achievements via-à-vis the mandatory results and

[1] Sections 7.1-7.3 are to be kept without changes in all Twinning fiches.

provide precise recommendations and corrective measures to be decided by in order to ensure the further progress.

8. Sustainability

At policy level, the project is expected to have impact on the national legislation, namely to contribute in its alignment to EU acquis an in the area of fight against organised crime, terrorism and cyber crime. As such, the action will lead to improvement of the legislation of the country as well as practices that will lead to better organisation and functioning of the institutions responsible in these three areas.

From technical point of view, the action envisages preparation of documents for inter-institutional cooperation that will enable joint coordination and comprehensive approach in the fight against cybercrime, organized crime, terrorism, radicalization, and violent extremism. Several documents will be prepared and upgraded in line with the EU and international best practices. Number of trainings will be delivered among the stakeholders. These activities will contribute for strengthening of the capacities of the Beneficiary institution and other stakeholders on operational level for conducting crime investigations for crimes related to cybercrime, organized crime, terrorism, radicalization, and violent extremism.

9. Crosscutting issues *(equal opportunity, environment, climate etc…)*

The cross-cutting issues will be addressed throughout the project. Throughout the project cycle, in particular when developing project working plan, state actors specifically addressing (one of) the cross cutting issues shall be consulted.

The main-streaming of the cross-cutting issues is regarded on two different levels: (a) Ensuring that the internal policies, structure or operating procedures of the beneficiary agency will conform to and promote the relevant principles outlined per section below and (b) ensuring that the products, outputs produced by the beneficiaries (e.g. guidelines, manuals etc.) will conform to and promote the relevant principles outlined per section below.

The following cross-cutting issues should be addressed:

Environmental Protection, Climate Change and Biodiversity

The project strengthens the rule of law framework by enhancing the capabilities of law enforcement services to combat criminality and safeguard citizens' security and public order. Additionally, it acknowledges the potential risks posed by cyber-attacks, which can lead to losing control over critical equipment and warning systems, harming human health and the environment. These risks encompass catastrophic spills, waste discharges, and air emissions, which may trigger fires, explosions, and the release of hazardous materials, causing significant bodily injury, property damage, environmental remediation expenses, and liability claims. As a result, this project contributes to improving risk control, management, and prevention measures to protect the environment.

Minority and Vulnerable Groups

The relevant legislation related to protection of the minorities and vulnerable groups and other related issues is developed and implemented in the country. The project will ensure that minorities and vulnerable groups needs will be considered as an analytical instrument from programme design onwards. The project will be sensitive and will ensure minorities and vulnerable groups to benefit in all project's activities and deliverables.

Equal opportunities and gender mainstreaming

The relevant legislation related to the equal opportunity issues is developed and implemented in the country. The project will ensure that gender needs will be considered as an analytical instrument from programme design onwards. The project will be gender sensitive and ensure access of woman to its benefits in all project activities and deliverables. All indicators will be disaggregated by gender.

Good Governance and Fight against Crime

Considering the overall objective and the project purpose, this project will contribute for more effective conducting of criminal cases against organised crime, terrorism and cybercrime that will contribute for establishing good governance and increasing the level of rule of law in the Republic of North Macedonia.

10. Conditionality and sequencing

Projects implemented through twinning require full commitment and involvement on behalf of senior level officials of the beneficiary institution. Therefore, the leadership of the Ministry commits itself to provide adequate staff and other resources and support to the twinning partner as well as to introduce the institutional changes identified as needed for the successful implementation of the project.

During the work on the project, access of the twinning partners to all necessary management levels will be ensured.

Conditionalities

- Appointment of counterpart personnel by the final beneficiary before the launch of the call of proposal and guaranteeing the continuity of the appointed and trained staff;
- Allocation of working space and facilities by the final beneficiary within the premises of the beneficiaries before contract signature;
- Participation by the final beneficiary in the selection process as per EU regulations;
- Organisation, selection and appointment of members of working groups, steering and coordination committees, seminars by the final beneficiaries;
- Active engagement for the use and application of project outputs.

11. Indicators for performance measurement

The measurable indicators for component 1 are:

Sub-result 1.1: Strategic and organisational framework strengthened

1) Analysis conducted of the legal and regulatory framework covering joint investigations, organised crime, terrorism, money laundering and inter-agency cooperation and Report prepared;
2) Written recommendations for harmonisation of national legislation and procedures with the relevant EU acquis and international standards prepared;
3) Gap analysis of current inter-institutional cooperation mechanisms in the area of fight against organised crime, terrorism and money laundering conducted, and Operational Cooperation Roadmap prepared;
4) Inter-Agency Intelligence Cooperation Framework prepared, adopted and operationalised by the relevant beneficiary institutions;
5) Unified intelligence reporting formats (operational, strategic and cross-border templates) developed and harmonised with Europol SIENA standards;
6) Real-time communication protocol for priority intelligence and investigation cases developed, approved and introduced for operational use;
7) Number of Joint Analytical Teams (JATs) established and operationalised for priority organised crime investigations;
8) Recommendations for strengthening interoperability, secure information exchange and access to national and international databases prepared;
9) Proposals for strengthening organisational structures, specialised units, IT systems and analytical capacities prepared;

Sub-result 1.2: Operational and investigative capacities strengthened

1) Review and assessment of existing operational procedures, investigative methodologies and standard operating procedures conducted, with recommendations for alignment with EU best practices prepared;
2) Number of operational procedures, manuals, guidelines or investigative methodologies revised or developed in line with EU standards and operational requirements;
3) Training needs assessment covering criminal intelligence, investigative techniques, digital forensics, HUMINT, financial investigations, evidence collection and cyber-hybrid crime conducted and report prepared;
4) Comprehensive training curricula and training materials for law enforcement officers developed;
5) Number of specialised trainings, workshops or practical exercises delivered to law enforcement officers and relevant practitioners;
6) Number of representatives of law enforcement institutions trained in modern investigative and analytical methods;
7) Operational and analytical capacities strengthened in the areas of trafficking in human beings, migrant smuggling, drug trafficking and firearms trafficking through specialised capacity-building activities and operational guidance;
8) Methodological guidance and operational tools for distinguishing trafficking in human beings from migrant smuggling developed in line with EU standards and disseminated to relevant institutions;
9) Recommendations for improving victim-sensitive approaches, evidence collection procedures and cross-border operational cooperation prepared;
10) Number of practical exercises, case simulations or joint operational activities conducted to strengthen operational readiness and inter-agency coordination in organised crime investigations.

Sub-result 1.3: National and international cooperation strengthened

1) Assessment of existing national and international cooperation frameworks and operational coordination mechanisms conducted, with recommendations for improvement prepared;
2) Cooperation mechanisms and coordination arrangements with EU Member States, Europol, Eurojust, Frontex, FIUs, ARO platforms and relevant international networks reviewed and strengthened;
3) Number of operational coordination meetings, workshops or technical exchanges organised with EU agencies, Member States and international partners;
4) Procedures and protocols for secure and timely information exchange between national law enforcement institutions and international partners developed;
5) Recommendations for strengthening interoperability and operational cooperation in cross-border investigations prepared;
6) Number of joint operational exercises, simulation exercises or coordinated operational activities implemented;
7) Number of representatives of beneficiary institutions that participated in cross-border cooperation, coordination or joint operational activities;
8) Operational coordination arrangements for joint investigations and cross-border actions strengthened through practical cooperation activities and exchange of operational experience;
9) Collection of good practices and lessons learned from national and international cooperation activities prepared and integrated into institutional procedures, operational guidelines or training materials;

The measurable indicators for component 2 are:

Sub-result 2.1: Operational capacities for cyber threat prevention, detection and response strengthened

1) Needs assessment on cybersecurity governance, operational coordination and technical infrastructure conducted, with recommendations prepared;
2) Operational procedures, escalation protocols and cyber incident response arrangements reviewed and aligned with EU best practices;
3) Operational procedures, incident response protocols or technical guidelines developed or updated for cyber incident prevention, detection and response;
4) Cooperation mechanisms between CSIRTs, law enforcement authorities, prosecutors and relevant stakeholders strengthened through formalised coordination procedures and operational arrangements;
5) Capacities for cybercrime investigation, digital forensics, electronic evidence handling and cyber incident attribution strengthened through specialised operational support and practical activities;
6) Number of specialised trainings, workshops or technical exercises delivered in the area of cyber incident response, cybercrime investigation and digital forensics;
7) Number of representatives of relevant institutions trained in cyber threat prevention, detection, investigation and response;
8) Number of joint simulation or operational cyber exercises conducted to test inter-agency coordination, operational readiness and response capacities;

9) Recommendations for improving operational coordination, cyber incident escalation and crisis response mechanisms prepared.

Sub-result 2.2: National, regional and international cyber cooperation strengthened

1) National Single Point of Contact (SPOC) for international cyber cooperation established and operationalised;
2) Assessment of existing national and international cyber cooperation and information-sharing mechanisms conducted, with recommendations for improvement prepared;
3) Secure communication channels and procedures for cyber threat intelligence exchange and incident information sharing between cybersecurity institutions and law enforcement agencies established and operationalised;
4) Number of coordination meetings, workshops or technical exchanges organised with EU and international cyber networks, agencies and organisations;
5) Operational cooperation mechanisms with EU and international cyber partners strengthened through participation in joint activities, information exchange and coordination initiatives;
6) Joint coordination arrangements for cross-border cyber incident response reviewed, tested and improved;
7) Number of representatives of cybersecurity institutions and LEAs participate in international cooperation, coordination or information-sharing activities;
8) Staff capacities strengthened for international cyber cooperation, cyber diplomacy and operational information exchange through targeted training and practical exercises;

Sub-result 2.3: Cybersecurity awareness, training and capacity building strengthened

1) Training needs assessment conducted for relevant institutions covering cybercrime investigation, digital evidence handling, cyber incident response and cybersecurity awareness;
2) Training curricula, operational guidance and training materials developed and approved by the beneficiary institutions;
3) Number of training sessions, workshops or simulation activities delivered for relevant institutions and stakeholders;
4) Number of representatives of public institutions, law enforcement agencies and relevant stakeholders trained in cybersecurity-related topics;
5) Awareness-raising activities on cyber hygiene, cyber threats and protection of critical infrastructure conducted at national and institutional level;
6) Practical exercises, workshops and simulation activities conducted involving cybersecurity institutions, law enforcement agencies and other relevant stakeholders;
7) Operational guidance, manuals and good practices aligned with EU cybersecurity standards developed and disseminated to relevant institutions;
8) Recommendations for strengthening institutional cybersecurity awareness and operational preparedness prepared.

Sub-result 2.4: National cyber risk assessment and preparedness strengthened

1) National cyber risk assessment conducted in line with EU methodologies and relevant international standards, with participation of law enforcement agencies and relevant stakeholders;

2) Report containing cyber threat and risk assessment findings with recommendations and priority actions prepared;
3) Institutional capacities strengthened to integrate cyber risk assessment findings into strategic planning, prioritisation and decision-making processes;
4) National coordination and response arrangements for major cyber incidents developed and aligned with relevant national and EU frameworks;
5) Number of scenario-based cyber incident response exercises conducted to test national preparedness, coordination and resilience capacities;
6) Public awareness initiatives on cyber resilience, preparedness and response to cyber threats implemented;
7) Recommendations for improving national cyber preparedness, crisis coordination and operational resilience prepared;
8) Good practices and lessons learned from cyber risk assessments and preparedness exercises integrated into institutional procedures and response frameworks.

12. Facilities available

The Beneficiary commits itself to make available free of any charge for the project:

- Office facilities for the RTA and the RTA assistants for the entire duration of their secondment, with a level of equipment at least comparable to that in use in the Beneficiary administration;
- Adequate conditions for the short-term experts to perform their work while on mission to the Beneficiary;
- Training and conference venues, catering if appropriate and presentation and interpretation equipment.

ANNEXES TO PROJECT FICHE

1. The Simplified Logical framework matrix as per Annex C1a (compulsory)
2. Organigram of the BC institution: https://mvr.gov.mk/mk-MK/ministerstvo/za-biroto

Annex C1a : Simplified Logical Framework

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
Overall Objective	The overall objective of this project is to improve the security architecture of North Macedonia.	Achieved progress of the Republic of North Macedonia in completing the security architecture in the area of fight against organised crime and terrorism and cyber-crime.	EC Progress Report for the Republic of North Macedonia	Lack of commitment from the managers/high level decision making of the beneficiary institutions and relevant personnel to participate in the activities of the project;	Government maintains its efforts to adopt the Union acquis and to pave the way for final EU accession

Specific (Project) Objective(s)	The specific objective is to significantly strengthen the capacity of national institutions to detect, investigate, prosecute, and prevent security threats and risks related to cybercrime, organized crime, terrorism, radicalization, and violent extremism.	Number of staff trained Increased number of threat reports identified by national institutions Outreach programs conducted on cyber security	Internal project reports List of participants and training reports including agendas, materials used, and evaluation forms Data on the threat reports identified Event agendas and attendance logs from outreach activities (seminars, webinars, school/university programs). Promotional materials	Changes in senior management Fluctuation of staff involved in the project Staff unavailable to provide support to MS experts and to participate in project activities Trained staff leave its workplace shortly after the project end	The beneficiary country continuously supports and MS project in the implementation of project activities Organizational, technical and infrastructural capacities necessary for implementation of the project in place and available Human resources for implementation of the project in place and available Capability and active role of relevant stakeholders to implement project results into practice
Component 1: Strengthening the strategic and operational capacities of law enforcement agencies to prevent and combat organised crime and security threats in line with EU and international standards					
Mandatory result 1 National strategic, operational and investigative capacities of law enforcement agencies strengthened to effectively prevent and combat organised crime, including migrant smuggling, trafficking in human beings, drug trafficking, firearms trafficking, and related security threats, in line with EU acquis and international standards					

Sub-result 1.1	1) National legal, institutional and organisational frameworks for combating organised crime are reviewed and recommendations prepared for alignment with EU acquis and international standards; 2) Strategic coordination and planning capacities for joint law enforcement action are strengthened; 3) Inter-agency cooperation and information exchange mechanisms are enhanced, including cooperation with law enforcement agencies (LEAs); 4) Institutional needs and capacity gaps are identified with recommendations for strengthening organisational structures, specialised units, and interoperability, including IT and data management capacities;	1) Analysis conducted of the legal and regulatory framework covering joint investigations, organised crime, terrorism, money laundering and inter-agency cooperation and Report prepared; 2) Written recommendations for harmonisation of national legislation and procedures with the relevant EU acquis and international standards prepared; 3) Gap analysis of current inter-institutional cooperation mechanisms in the area of fight against organised crime, terrorism and money laundering conducted, and Operational Cooperation Roadmap prepared; 4) Inter-Agency Intelligence Cooperation Framework prepared, adopted and operationalised by the relevant beneficiary institutions; 5) Unified intelligence reporting formats (operational, strategic and cross-border templates) developed and harmonised with Europol SIENA standards;	Report of the conducted analysis; Recommendations report; Gap analysis; Operational Cooperation Roadmap; Adopted Inter-Agency Intelligence Cooperation Framework and institutional decisions/approvals for its implementation; Unified intelligence reporting formats (operational, strategic and cross-border templates); Approved real-time communication protocol, internal operational procedures and records of operational use; Operational reports and records of joint investigations; Recommendations report;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

	5) Proposals are developed to improve secure information exchange and interoperability with relevant national and international systems and databases.	6) Real-time communication protocol for priority intelligence and investigation cases developed, approved and introduced for operational use; 7) Number of Joint Analytical Teams (JATs) established and operationalised for priority organised crime investigations; 8) Recommendations for strengthening interoperability, secure information exchange and access to national and international databases prepared; 9) Proposals for strengthening organisational structures, specialised units, IT systems and analytical capacities prepared	Proposals for strengthening organisational structures, specialised units, IT systems and analytical capacities.		

Sub-result 1.2	1) Operational procedures and investigative practices are reviewed and improved in line with EU best practices; 2) Capacities in modern investigative methods and analytical approaches, including digital forensics, HUMINT, and financial investigations, are strengthened; 3) Training needs are identified and training curricula developed covering criminal intelligence, investigative techniques, evidence collection, and cyber-hybrid crime; 4) Targeted trainings are delivered to strengthen operational and analytical capacities of law enforcement officers; 5) Operational capacities are strengthened for the investigation and prosecution of organised crime, including trafficking in human beings, migrant smuggling, drug trafficking, and	1) Review and assessment of existing operational procedures, investigative methodologies and standard operating procedures conducted, with recommendations for alignment with EU best practices prepared; 2) Number of operational procedures, manuals, guidelines or investigative methodologies revised or developed in line with EU standards and operational requirements; 3) Training needs assessment covering criminal intelligence, investigative techniques, digital forensics, HUMINT, financial investigations, evidence collection and cyber-hybrid crime conducted and report prepared; 4) Comprehensive training curricula and training materials for law enforcement officers developed; 5) Number of specialised trainings, workshops or practical exercises delivered to law enforcement officers and relevant practitioners;	Review and assessment reports of existing operational procedures, investigative methodologies and standard operating procedures conducted; Recommendations for alignment with EU best practices prepared; SOPs, manuals, guidelines and methodologies prepared; Training Needs Assessment (TNA) report; Training curricula; Training modules and lesson plans; Training manuals and handbooks; Learning materials and presentations; Training reports; Agendas and programmes; Attendance sheets; Workshop and exercise reports;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

	firearms trafficking, with a focus on victim-sensitive and cross-border cooperation approaches; 6)Methodological guidance is developed to support the distinction between trafficking in human beings and migrant smuggling in line with EU standards.	6) Number of representatives of law enforcement institutions trained in modern investigative and analytical methods; 7) Operational and analytical capacities strengthened in the areas of trafficking in human beings, migrant smuggling, drug trafficking and firearms trafficking through specialised capacity-building activities and operational guidance; 8) Methodological guidance and operational tools for distinguishing trafficking in human beings from migrant smuggling developed in line with EU standards and disseminated to relevant institutions; 9) Recommendations for improving victim-sensitive approaches, evidence collection procedures and cross-border operational cooperation prepared; 10) Number of practical exercises, case simulations or joint operational activities conducted to strengthen operational readiness and inter-agency coordination in organised crime investigations.	Participant lists; Certificates of completion; Evaluation forms; Operational guidance documents; Post-training evaluations Institutional progress reports; Methodological guidance document; Operational tools/checklists/indicators Recommendations report; Exercise reports; Scenario documents and exercise plans Evaluation and after-action reports Attendance lists Joint operation reports		

Sub-result 1.3	1) Cooperation frameworks with EU Member States, EU agencies (including Europol, Eurojust, Frontex), FIUs, ARO platforms, and relevant international networks are strengthened; 2) Cooperation mechanisms between national law enforcement institutions and LEAs are enhanced, including secure and timely information exchange; 3)Operational coordination arrangements for cross-border investigations and joint actions are strengthened; 4) Joint operational exercises and coordination activities are implemented to enhance readiness and cooperation;	1) Assessment of existing national and international cooperation frameworks and operational coordination mechanisms conducted, with recommendations for improvement prepared; 2) Cooperation mechanisms and coordination arrangements with EU Member States, Europol, Eurojust, Frontex, FIUs, ARO platforms and relevant international networks reviewed and strengthened; 3) Number of operational coordination meetings, workshops or technical exchanges organised with EU agencies, Member States and international partners; 4) Procedures and protocols for secure and timely information exchange between national law enforcement institutions and international partners developed; 5) Recommendations for strengthening interoperability and operational cooperation in cross-border investigations prepared;	Assessment report; Review report of cooperation frameworks; Recommendations report; Review reports and assessment findings; Cooperation agreements, protocols or arrangements developed/revised; Records of consultations with EU and international partners; Institutional progress reports; Agendas and programmes; Attendance lists; Workshop reports; Technical exchange reports; Procedures and protocols; Standard operating procedures (SOPs); Information exchange guidelines;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

	5) Good practices and lessons learned from national and international cooperation are integrated into institutional procedures and frameworks.	6) Number of joint operational exercises, simulation exercises or coordinated operational activities implemented; 7) Number of representatives of beneficiary institutions that participated in cross-border cooperation, coordination or joint operational activities; 8) Operational coordination arrangements for joint investigations and cross-border actions strengthened through practical cooperation activities and exchange of operational experience; 9) Collection of good practices and lessons learned from national and international cooperation activities prepared and integrated into institutional procedures, operational guidelines or training materials;	Recommendations report; Exercise plans and scenarios; Operational activity reports; Exercise evaluation reports; After-action review reports Attendance records; Participant lists; Attendance records; Mission reports; Study visit reports; Joint investigation coordination reports; Exchange-of-experience reports; Institutional progress reports; Compendium of good practices and lessons learned; Training materials and manuals; Revised institutional procedures and guidelines;		

Component 2: Strengthening national cybersecurity resilience
Mandatory Result 2: National cybersecurity resilience and cybercrime response capacities are enhanced through improved operational procedures, institutional coordination, information sharing, technical capabilities, and awareness, in line with EU cybersecurity standards and best practices

Sub-result 2.1	1) Needs assessment conducted and recommendations prepared to strengthen cybersecurity governance, operational coordination, and technical infrastructure; 2) Operational procedures, escalation protocols, and cyber incident response arrangements developed and improved in line with EU best practices; 3) Cooperation mechanisms between CSIRTs, law enforcement authorities, prosecutors, and relevant stakeholders strengthened for coordinated cyber incident response and cybercrime investigation;	1) Needs assessment on cybersecurity governance, operational coordination and technical infrastructure conducted, with recommendations prepared; 2) Operational procedures, escalation protocols and cyber incident response arrangements reviewed and aligned with EU best practices; 3) Operational procedures, incident response protocols or technical guidelines developed or updated for cyber incident prevention, detection and response; 4) Cooperation mechanisms between CSIRTs, law enforcement authorities, prosecutors and relevant stakeholders strengthened through formalised coordination procedures and operational arrangements; 5) Capacities for cybercrime investigation, digital forensics, electronic evidence handling and cyber incident attribution strengthened through specialised operational support and practical activities;	Needs assessment report; Recommendations report; Review and assessment reports; Gap analysis against EU standards and best practices; Recommendations report; Operational procedures and protocols; Incident response plans and guidelines; Technical manuals and handbooks; Cooperation agreements, protocols or memoranda; Coordination procedures and SOPs; Institutional progress reports; Operational support reports; Technical assistance mission reports; Capacity-building activity reports; Practical exercise reports; Institutional assessments and progress reports;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

	4) Capacities strengthened for cybercrime investigation, digital forensics, handling of electronic evidence, and incident attribution; 5) Targeted trainings and operational exercises delivered to enhance readiness and response to cyber threats; 6) Joint simulation and operational exercises conducted to test inter-agency coordination and response capabilities.	6) Number of specialised trainings, workshops or technical exercises delivered in the area of cyber incident response, cybercrime investigation and digital forensics; 7) Number of representatives of relevant institutions trained in cyber threat prevention, detection, investigation and response; 8) Number of joint simulation or operational cyber exercises conducted to test inter-agency coordination, operational readiness and response capacities; 9) Recommendations for improving operational coordination, cyber incident escalation and crisis response mechanisms prepared.	Training and workshop reports; Agendas and programmes; Attendance lists; Exercise reports; Training evaluation forms; Participant lists; Attendance records; Certificates of completion; Exercise plans and scenarios; Simulation reports; After-action review reports; Exercise evaluation reports; Recommendations report;		

Sub-result 2.2	1) National Single Point of Contact (SPOC) for international cyber cooperation established and operationalised; 2) Information-sharing mechanisms between national cybersecurity institutions and law enforcement agencies (LEAs) strengthened; 3) Cooperation with EU and international cyber networks and organisations further developed and enhanced; 4) Secure communication channels and procedures for cyber threat intelligence and incident information exchange between cybersecurity institutions and LEAs established and operationalised;	1) National Single Point of Contact (SPOC) for international cyber cooperation established and operationalised; 2) Assessment of existing national and international cyber cooperation and information-sharing mechanisms conducted, with recommendations for improvement prepared; 3) Secure communication channels and procedures for cyber threat intelligence exchange and incident information sharing between cybersecurity institutions and law enforcement agencies established and operationalised; 4) Number of coordination meetings, workshops or technical exchanges organised with EU and international cyber networks, agencies and organisations; 5)Operational cooperation mechanisms with EU and international cyber partners strengthened through participation in joint activities, information exchange and coordination initiatives;	Government decision or institutional act establishing the SPOC; Organisational charts and designation documents; Operational procedures and workflows; Assessment report; Review report on cooperation mechanisms; Recommendations report; Procedures and protocols; Technical documentation and system deployment records; SOPs for information exchange; User/access records; Operational testing reports; Agendas and programmes; Attendance lists; Workshop reports; Technical exchange reports; Cooperation agreements, MoUs or working arrangements; Institutional progress reports;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

	5) Joint coordination mechanisms for cross-border cyber incident response strengthened; 6) Staff capacities enhanced for effective international cooperation and information exchange during cyber incidents.	6) Joint coordination arrangements for cross-border cyber incident response reviewed, tested and improved; 7) Number of representatives of cybersecurity institutions and LEAs participate in international cooperation, coordination or information-sharing activities; 8) Staff capacities strengthened for international cyber cooperation, cyber diplomacy and operational information exchange through targeted training and practical exercises;	Assessment reports; Exercise reports and testing documentation; Updated procedures and coordination protocols; Recommendations and improvement plans; Participant lists; Attendance records; Mission reports; Training reports; Agendas and curricula; Attendance sheets; Exercise reports; Training evaluation forms and certificates.		

Sub-result 2.3	1) Training needs assessment conducted and training curricula developed for relevant institutions; 2) Training programmes delivered on cybercrime investigation, digital evidence handling, and cyber incident response; 3) Awareness-raising activities implemented on cyber hygiene, cyber threats, and protection of critical infrastructure; 4) Practical exercises, workshops, and simulation activities conducted involving relevant stakeholders; 5) Operational guidance and good practices aligned with EU cybersecurity standards developed and applied.	1) Training needs assessment conducted for relevant institutions covering cybercrime investigation, digital evidence handling, cyber incident response and cybersecurity awareness; 2) Training curricula, operational guidance and training materials developed and approved by the beneficiary institutions; 3) Number of training sessions, workshops or simulation activities delivered for relevant institutions and stakeholders; 4) Number of representatives of public institutions, law enforcement agencies and relevant stakeholders trained in cybersecurity-related topics; 5) Awareness-raising activities on cyber hygiene, cyber threats and protection of critical infrastructure conducted at national and institutional level;	Training Needs Assessment (TNA) report; Survey results and questionnaires; Stakeholder consultation reports; Training curricula; Training modules and lesson plans; Operational guidance documents; Training manuals and handbooks; Training and workshop reports; Agendas and programmes; Attendance sheets; Simulation exercise reports; Evaluation forms;	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

		6) Practical exercises, workshops and simulation activities conducted involving cybersecurity institutions, law enforcement agencies and other relevant stakeholders; 7) Operational guidance, manuals and good practices aligned with EU cybersecurity standards developed and disseminated to relevant institutions; 8) Recommendations for strengthening institutional cybersecurity awareness and operational preparedness prepared	Participant lists; Attendance records; Certificates of completion; Awareness campaign reports; Communication and outreach materials; Event agendas and participant records; Publications, brochures and online materials; Media coverage and dissemination records; Exercise plans and scenarios; Workshop reports; Simulation activity reports; Attendance lists; After-action review and evaluation reports; Guidance documents and manuals; Compendium of good practices; Recommendations report.		

Sub-result 2.4	1) National cyber risk assessment conducted in line with EU methodologies, with the involvement of law enforcement agencies (LEAs) in the threat assessment process; 2) Institutional capacities strengthened to integrate risk assessment findings into strategic planning, prioritisation, and decision-making processes; 3) National coordination and response arrangements for major cyber incidents developed, tested, and aligned with relevant national and EU frameworks; 4) Public awareness initiatives and scenario-based exercises implemented to strengthen cybersecurity preparedness and resilience.	1) National cyber risk assessment conducted in line with EU methodologies and relevant international standards, with participation of law enforcement agencies and relevant stakeholders; 2) Report containing cyber threat and risk assessment findings with recommendations and priority actions prepared; 3) Institutional capacities strengthened to integrate cyber risk assessment findings into strategic planning, prioritisation and decision-making processes; 4) National coordination and response arrangements for major cyber incidents developed and aligned with relevant national and EU frameworks; 5) Number of scenario-based cyber incident response exercises conducted to test national preparedness, coordination and resilience capacities; 6) Public awareness initiatives on cyber resilience, preparedness and response to cyber threats implemented;	National cyber risk assessment; Methodology and assessment framework documentation; Records of stakeholder consultations and workshops; Attendance lists and participation records; Cyber threat and risk assessment report; Recommendations and action plan document; Executive summary and policy brief; Strategic planning documents revised based on assessment findings; Institutional action plans; Progress and implementation reports; National coordination procedures and response plans; Crisis management protocols; Standard Operating Procedures (SOPs);	Lack of commitment Insufficient human and technical resources for daily work with the Twinning Partner	Availability of sufficient relevant information Active participation of the personnel

		7) Recommendations for improving national cyber preparedness, crisis coordination and operational resilience prepared; 8) Good practices and lessons learned from cyber risk assessments and preparedness exercises integrated into institutional procedures and response frameworks.	Alignment and compliance assessment reports; Exercise plans and scenarios; Exercise reports; Attendance records; Evaluation reports; After-action review reports; Awareness campaign reports; Communication and outreach materials; Event reports and attendance records; Media coverage and dissemination records; Recommendations report; Guidance documents; Assessment and evaluation reports; Lessons learned and Good practice compendium; Revised procedures, SOPs and response frameworks.		