EN

ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX 3

to the Commission Implementing Decision on the financing of the multiannual action plan in favour of the Republic of Kenya for 2023-2024

Action Document for Strengthening Kenya's security and cybersecurity

MULTIANNUAL PLAN
This document constitutes the multiannual work programme within the meaning of Article 110(2) of the Financial Regulation, within the meaning of Article 23 of the NDICI-Global Europe Regulation.

1 SYNOPSIS

1.1 Action Summary Table

1. Title **CRIS/OPSYS business reference** **Basic Act**	**Strengthening Kenya's security and cybersecurity** OPSYS number: ACT-61794 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe)/ Overseas Association Decision/European Instrument for International Nuclear Safety Cooperation Regulation
2. Team Europe Initiative	Yes, part of the Team Europe Initiative on Human Centred Digitalisation Kenya
3. Zone benefiting from the action	The action shall be carried out in Kenya
4. Programming document	Multi-annual Indicative Programme for Kenya 2021-2027[1]
5. Link with relevant MIP(s) objectives / expected results	Specific objective: Reduced threats to Kenya's national security and stability, including maritime security Expected result 3.2a: Drivers of conflict are addressed by supporting local peace structures and livelihoods Expected result 3.2b: Kenya's capacity to respond to violent extremism (PCVE) and Counter-terrorism (CT), and emerging threats contributing to instability, is strengthened at national and county level
PRIORITY AREAS AND SECTOR INFORMATION	
6. Priority Area(s), sectors	MIP Priority Area 3: Democratic Governance, Peace and Stability MIP sector: 3.2. Conflict, peace and security

[1] Decision C(2021) 9088 Final, dated 14/12/2021, adopting a Multiannual Indicative Programme for the Republic of Kenya for the period 2021-2027

7. Sustainable Development Goals (SDGs)	Main SDG: SDG 16 Peace, Justice and Strong Institutions Other significant SDGs: SDG 5 Gender equality, SDG 9 Build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation SDG 10 Reduced inequalities, SDG 17 Partnerships for the Goals			
8 a) DAC code(s)	152 Conflict Peace and Security (80%) 15180 Ending violence against women and girls (20%)			
8 b) Main Delivery Channel	Central Government - 12001, Member State Agency -11003, Non-Governmental Organisations, NGOs and Civil Society-20000			
9. Targets	☐ Migration ☐ Climate ☐ Social inclusion and Human Development ☒ Gender ☐ Biodiversity ☐ Education ☒ Human Rights, Democracy and Governance			
10. Markers (from DAC form)	**General policy objective** @	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	x
	Aid to environment @	x	☐	☐
	Gender equality and women's and girl's empowerment	☐	x	☐
	Reproductive, maternal, new-born and child health	x	☐	☐
	Disaster Risk Reduction @	x	☐	☐
	Inclusion of persons with Disabilities @	☐	x	☐
	Nutrition @	x	☐	☐
	RIO Convention markers	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity @	x	☐	☐
	Combat desertification @	x	☐	☐
	Climate change mitigation @	x	☐	☐
	Climate change adaptation @	x	☐	☐
11. Internal markers and Tags:	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	Digitalisation @	☐	x	☐
	digital connectivity	YES x	NO ☐	

	digital governance digital entrepreneurship digital skills/literacy digital services	x ☐ x x	☐	
	Connectivity @	x	☐	☐
	digital connectivity energy transport health education and research	YES ☐ ☐ ☐ ☐	NO x x x x	
	Migration @	x	☐	☐
	Reduction of Inequalities @	x	☐	☐
	Covid-19	x	☐	☐

BUDGET INFORMATION

12. Amounts concerned

Budget line(s) (article, item): BGUE-B2024-14.020121-C1-INTPA

Total estimated cost: EUR 10 000 000

Total amount of EU budget contribution: EUR 10 000 000

The contribution is for an amount of EUR 10 000 000 from the general budget of the European Union for 2024, subject to the availability of appropriations for the respective financial years following the adoption of the relevant annual budget, or as provided for in the system of provisional twelfths.

The expected contributions of EU partners to the Team Europe Initiative on Digitalisation amount to EUR 432 150 000, with the following indicative contr per Member States (in million EUR):

BE	DE	EIB	FI	FR	IT	EU	NL	SE	SK
13.1	28	104	tbc	30	3.5	109	132	12.5	0.05

MANAGEMENT AND IMPLEMENTATION

13. Type of financing

Direct management through Grants

Indirect management with the entity (-ies) to be selected in accordance with the criteria set out in section 4.3.2 and 4.3.3.

1.2 Summary of the Action

This action will work to reinforce two interconnected strands of security: (1) Preventing and countering violent extremism (PCVE); (2) Strengthening the resilience of the cybersecurity ecosystem. By enabling a more secure environment, including in the digital space, this action directly contributes to the EU-Kenya Green and Digital Partnership under the Global Gateway. Expanding on existing bilateral and regional cooperation, this action will address two key priorities agreed in the context of the EU-Kenya Strategic

Dialogue preventing violent extremism and cybersecurity delivered through the means of three components.

1) The first component will support the capacities of key national and county-level authorities in the implementation of the national strategy on PCVE and will follow up the dialogue on counter-terrorism between Kenya and the EU. The action will incorporate human-rights and gender transformative capacity building of the law enforcement combined with active disengagement activities for youth (men and women) living in the most vulnerable situations, among others.

2) The second component will work with local partners to strengthen community resilience to violent extremism. This component support initiatives led by, and benefiting, local communities that empower women, girls, boys, men and in a larger sense, persons living in vulnerable situations – including internally displaced persons (IDPs) and refugees - who are more at risk of radicalisation.

3) The third component will strengthen the resilience of the Cybersecurity ecosystem through support to the implementation of the new national cybersecurity strategy. It will focus inter alia on the critical infrastructures resilience, capacity building, awareness raising, peer-to-peer exchanges with similar Member States agencies, strengthening the Kenya Computer Incident Response Team (KE-CIRT) and supporting cooperation and collaboration at international level in line with international conventions.

The action also meets the terms of the Sustainable Development Goal (SDG) (16) by promoting peaceful and inclusive societies for sustainable development, providing access to justice for all and building effective, accountable, and inclusive institutions at all levels. It also contributes to the Action Plan for the implementation of the Strategic Framework highlighting issues affecting the European Union (EU) interests in the region that have become more pronounced and critical over the last years. Importantly, the action complies with the EU and Kenya's commitment to Counter Terrorism and Prevent and Counter Violent Extremism (CT-PCVE), related UN Security Council resolutions (including UNSCR 1325 on Women Peace and Security[2]) and conventions as well as the UN action plan on preventing violent extremism.

The Action aligns with the EU-AU Digital compact. It is in support of Global Gateway roll out, notably the Global Gateway digital investment priority area and it is part of the Team Europe Initiative (TEI) on Human Centred Digitalisation. It will further support Kenya's digital agenda and EU's partnership with Africa on the transition to a digital age. It will notably strengthen the EU's engagement in the digital sector by assisting Kenya to implement its cybersecurity policy.

All components will be implemented in full complementarity with regional, trans-regional and global programmes and in coordination with European Commission services.

2 RATIONALE

2.1 Context

Kenya is East Africa's economic hub, a relatively stable democracy with an open civic space, and an important partner in multilateralism. However, the country is faced with chronic poverty and persistent

[2] Kenya launched its second National Action Plan in 2020 for the period 2020-2024. There have been some significant gains on the first Action Plan such as the Defence Ministry's gender policy, the first in the history of Kenya's military. The District Peace Committees (now County Peace Committees) had an average annual percentage increase of 5% in the number of women in the committees from 14% in 2014 to 29% in 2017. However the implementation of this Action Plan remains underfunded and weak.

inequalities (in particular gender inequality, i.e. almost a third of households are headed by women and are among the poorest)[3], ethnic divide and governance issues, including corruption and conflict.

Security threats and challenges have had considerable impact on Kenya's ability to achieve its development goals. Conflict and instability in the region, in addition to internal political and security challenges can fuel unrest, in particular when combined with tribalism, corruption, impunity and unresolved historical grievances. EU's strategic objectives in Kenya include promoting trade and investment, partnering on security for the stability of the country and the region, and addressing human development and inequalities. In May 2021, the **Council Conclusions on the Horn of Africa** have identified Kenya as a key partner for the EU and in June 2021, EU and Kenya (PEC Michel and President Kenyatta) launched a **Strategic Dialogue**. In January 2022, HRVP Borrell opened the Dialogue kick-off meetings covering 3 pillars: Peace and Security, Sustainable Development, Economics and Trade. In February 2023, a Senior Official Meeting held in Nairobi confirmed these strategic priorities. The 2022 EU Strategic Compass reiterates strategic lines of engagement with African countries, whereby ongoing conflicts, poor governance and terrorism across the continent affect the EU's security; stability in the Horn of Africa remains a major security imperative for the EU. Furthermore, the EU Action Plan on Human Rights and Democracy 2020-2024 provides guidance on minimising the risks of digital technologies, while the June 2020 Council Conclusions on Counterterrorism and Violent Extremism reiterates the importance and urgency of addressing these issues in the external actions and highlights that close cooperation with youth, children, women, civil society, human rights defenders and victims of terrorism remains a key to success. These priorities were reinforced at the Senior Official Meeting of the EU-Kenya Strategic Dialogue, held in Nairobi in February 2023.

Despite concerted efforts to counter violent extremism, radicalisation and recruitment continue to spread from the traditional hotspot counties into other regions of Kenya. This is exacerbated by the persistence of push and pull factors creating conditions favourable for radicalisation and recruitment. Beyond Kenya's borders, conflict and other factors have facilitated the expansion of Daesh and Al-Shabab threatening Kenya, and regional security. The risks of conflict, terrorism and violent extremism, in all their forms and irrespective of their origin, continue to evolve and pose a serious threat to Kenya's peace and security. Over the last two decades, terrorism has been on the rise with Al Shabaab increasing their attacks and radicalising the youth, including women and girls. In addition to women and girls being victims of attacks by Al Shabaab, there is also growing concern that there is an increase in female perpetrators.

A strong economy, a population of 54 million and a high level of usage of online services makes Kenya a favoured target for cyber threats. According to the African cyber threat Assessment report of October 2024, Kenya is with South Africa and Morocco one of the African countries most affected by cybercriminal activities. With more and more Kenyans connecting to the internet from mobile devices like phones and tablets, also comes the rise of mobile money and other economic transactions using digital technologies. This coupled with a lack of coherent legislation and regulatory frameworks, as well as inadequate cybersecurity measures in key sectors, is turning Kenya into a lucrative target for cyber criminals. In the space of democratic governance and participation, campaigns orchestrated by foreign regimes or interest groups relative to geopolitical interests are seen to sometimes counter democratic and universal values. Contributing to Kenya's cybersecurity will align with Global Gateway digital investment priority and principles democratic values and high standards security-focused principle.

Although increasing fast, the level of cybersecurity in Kenya has not been as fast as its digital transformation. Kenya has not signed nor ratified the African Union Malabo Convention on Cybersecurity and Personal data nor the Budapest convention on cybercrime and attacks have raised awareness in the general population (e.g. the Kaseya IT service by a ransomware group). In this context, this action will be an opportunity for the EU to promote an open, free, stable and secure cyberspace together with Kenyan

[3] Kenya CLIP.
[4] https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

counterparts. Notwithstanding the principle of the peaceful use of cyberspace, competition in this domain has strong security and defence implications, where the EU has an interest in establishing a strong and trusted partnership with Kenya. Support to the cybersecurity from other partners is relatively new and in incipit form. The proposed intervention will align closely with the regional intervention the Horn of Africa Initiative Project on cybersecurity. Furthermore, it will align as well with the support currently provided from the FCDO from the National Cyber Security Centre especially on the standard operating procedures.

The proposed action will thus build on the positive results of previous actions and its trusted cooperation with the Government of Kenya on preventing and countering violent extremism and counterterrorism by increased exchanges and deepened dialogue. Secondly, the action will initiate new partnerships between key national institutions in charge of cybersecurity and their EU Member states peers, with a view of **promoting European standards and policies in relation to cybersecurity**. This action will thus raise the profile of the EU in one of the two key regulatory issues of Kenya's digital transition (together with data protection) and will contribute to a more secure and enabling environment for ongoing and future planned investments, notably under the Global Gateway.

2.2 Problem Analysis

(1) Preventing and countering violent extremism (PCVE) at national level

Violent extremism mainly arising from Daesh and Al-Qaeda affiliates continues to affect socio-economic and political stability of the Country with sectors such as education, tourism, security, and transportation being the most affected. The 2021 Global Terrorism Index (GTI) ranked Kenya as a high-risk country with a 6.17 Impact of Terrorism. The threat of violent extremism is dynamic, fluid and rapidly changing; with radicalization and recruitment spreading from the initial hotspot counties in the Coastal and Northern Kenya regions to non-traditional counties in Central, Nairobi, Nyanza, Western and the Rift Valley. The existence of perceived or real political, religious, ideological, and social grievances within the communities have continued to be exploited by violent extremists' groups to radicalise, recruit, motivate and justify their actions.

Simultaneously, some Kenyans previously radicalised and recruited were deployed back into the country to execute high impact attacks as witnessed at the Westgate mall, Mpeketoni, Garissa University, 14-Riverside and Manda Bay attacks among others. The radicalisation threat in Kenya is further acerbated by the presence of violent extremist defectors from terrorist groups who inspire vulnerable and at-risk youth and women to support and perpetrate violent extremism activities. Empirical evidence indicates that terror groups exploit various avenues such as the internet, religious institutions, remand centres, prisons, and refugee camps to radicalise and recruit vulnerable individuals to join violent extremists' groups.

The implementation of the National Strategy of Countering Violent Extremism currently under review is resource intensive and requires collaboration of various actors among them, bilateral and multilateral partners. The review of the National Strategy is also being informed by the changes from the global level namely the United Nations Security Council Resolution (UNSCR) 1325 (2000). The Council Resolutions were ground-breaking in that it provided strong support for greater attention to the role of women in international peace and security. The UN Security Council fully recognizes the critical link between the Women, Peace and Security agenda as laid out in UNSCR 1325 and the role women could and should play in preventing violent extremism. As highlighted in the 2020 Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism[5], women can be particularly targeted and at risk of becoming victims, including through sexual and gender-based violence, as strategic objectives of terrorist groups.

(2) Preventing and countering violent extremism (PCVE) at community and individual level

[5] 2020 Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism

Marginalisation, exclusion and a lack of meaningful opportunities has led to grievances, which are broadly viewed as a combustible precursor for violence and violent extremism. Responses focused on security only, which neglect positive interactions with concerned communities, can contribute to grievances that ultimately drive conflict. This intervention aims to provide support to communities and government agencies in creating new opportunities and building stronger relationships which will result in a more peaceful and resilient society. To date, the Government of Kenya has not yet put in place a formal strategy to better manage and address tensions generated by actual or perceived marginalisation of communities. However, the Government of Kenya has taken positive steps to rebuild trust with its citizens by addressing their development needs and creating equal economic opportunities. The devolution of authority to the counties following the 2010 Constitution puts substantial responsibility for development to the counties. This intervention aims to directly support such efforts and generate new evidence, which will strengthen policy making and result in improved peace and development in marginalised regions Community actors are best placed to strengthen resilience, as they are closest to, and understand, the challenges in more detail. Local actors understand what drives recruitment and radicalisation to violent extremism in their communities and may have some of the solutions, but are often unable to access the funding they need to start to make a difference. Local P/CVE initiatives may be overlooked by traditional development funding, or they may lack the capacity to access and manage international donor funds where they are available. Communities need to fill this funding gap in a sound and sustainable manner, including investing in building the capacity of local initiatives to better serve their communities, to improve their potential to access and manage donor funds in the future, and to secure innovative partnerships that reinforce their stability. The intervention planned at community level will proactively engage across all activity areas wider society as represented by civil society organisations, including non-governmental organisations and community-based organisations such as youth organisations, movements and networks, women's and human rights organizations.

(3) Strengthening the resilience of the cybersecurity ecosystem

Kenya identifies cybersecurity as a national economic and security challenge. The most prevalent cybersecurity challenges in Kenya include exploitation of the new operating environment by adversaries to conduct disruptive operations on critical infrastructure. KE-CIRT, the institute responsible for national-level cyber incident detection and response, has noted a significant growth in the total threats detected, from 23 million in 2018 to 110 million in 2020. KE-CIRT statistics for the second quarter of 2021 show that ransomware, malware, and phishing attacks are the most common cybersecurity risks. This upward trend can be attributed to the rise in impersonation, online fraud, and online abuse cases arising from increased internet access and use. Data breaches, theft of proprietary information, financial damage, reputational loss, equipment destruction, distributed denial of service, illegal access to vital systems, and theft of personally identifiable information are all consequences of these attacks.

Most ICT users in Kenya have prioritised efficiency, cost and convenience while overlooking security during development and implementation. Interconnected ICTs have inherent vendor/manufacturer vulnerabilities that can be exploited by adversaries and expose Kenyan citizens, businesses and government to global threats. The Kenyan government recognises the **ICT sector as a key contributor and enabler in the attainment of the Vision 2030** to transform Kenya into a digital economy. Guided by key policy documents including the Digital Economy Blueprint, National ICT Policy and National Digital Masterplan, the ICT sector has continued to be a key contributor to the GDP and source of national economic growth. Kenya has adopted the National Cybersecurity Strategy in 2022, which provides direction for a unified approach in the implementation of cyber security for the public and private sector. Completed with a roadmap for implementation, the National Cybersecurity Strategy provides a conducive policy avenue for the implementation. Furthermore, Kenya enacted the Computer Misuse and Cybercrimes ACT -2018, which is currently the overarching law for protection of Critical Infrastructures and management of cybercrime in Kenya.

Identification of main stakeholders and corresponding institutional and/or organisational issues (mandates, potential roles, and capacities) to be covered by the action:

The **National Counter Terrorism Centre** (NCTC) established in 2004 to respond to the increasing threat of violent extremism and terrorism. The Centre is mandated by the Prevention of Terrorism Act (POTA 2012) to co-ordinate national counter-terrorism efforts to detect, deter and disrupt terrorism acts.

Law Enforcement Agencies - Protect communities against violent extremism

Regional bodies and regional partners (AU, IGAD, SADC) - Implementing Regional Strategy for preventing and countering violent extremism in East, Central and Southern Africa with a view to guiding the region in addressing the challenge of violent extremism in a more collaborative and cooperative manner. Sharing PCVE best practices, lessons learned and capacity building for PCVE actors.

Religious Institutions - To enhance inter-religious tolerance, social cohesion, counter violent extremists' ideologies and provide alternative narratives.

County Governments who are responsible for the coordination and implement County Action Plans, including the departments responsible for gender mainstreaming at county level.

County Engagement Forums (CEFs) and **Civil Society Organizations (CSOs)** both at national as well as at the local level (including human and women's rights as well as youth organisations).

The National Computer and Cybercrimes Coordination Committee (NC4) and the Secretariat as the national authority to spearhead and coordinate cybersecurity matters.

The National KE-CIRT/CC - this was established as a function of the Communication Authority in 2012. The Kenya Computer Incident Response Team Coordination Centre's role is to facilitate coordination and collaboration in response to cybersecurity incidents, in liaison with sector CIRTs and other local, regional and international cybersecurity management actors.

Academic institutions whose expertise includes cybersecurity, such as universities, research entities, think tanks, and independent experts and researchers.

Civil Society Organisations particularly youth, women's rights organisations and those with expertise in human rights, those engaging with different communities within society vulnerable to cyberattacks, those which engage directly with the public on cybersecurity related issues, as well as already engaging with local actors on prevention of violent extremism and radicalization issues (i.e. Strong Cities Network).

International and regional organisations whose mandate or expertise includes cybersecurity, such as ITU, the World Bank, CIVIPOL, Expertise France.

The technical community, including members of the incident response community, standard setting organisations, and domain name systems.

Private Sector including trade associations, particularly those from industries and sectors that are particularly vulnerable to cyber threats or who develop technology or provide services that enhance cybersecurity.

Final beneficiaries as rights holders are **communities** living in vulnerable situations (in particular women– including IDPs and young people in all their diversity), refugees at risk of recruitment and radicalisation to violent extremist agendas, in communities in Kenya that are both afflicted by violent extremism and lacking in government and civil society capacity to prevent violent extremism.

GCERF is solutions-oriented. Funding is provided to help launch, reinvest in, and extend successful local initiatives to build community resilience against violent extremist agendas, in a gender and age responsive way. As the reach of GCERF funding expands, the lessons learned in particular from our monitoring and

evaluation of PVE initiatives will contribute to good practices in this currently undeveloped, complex, and highly challenging field. Dissemination workshops will also be organised to this purpose.

3 DESCRIPTION OF THE ACTION

3.1 Objectives and Expected Outputs

The **Overall Objective** of this action is to reduce the number and intensity of incidents of violent extremism and cybersecurity attacks in Kenya.

The **Specific Objectives** (Outcomes) of this action are:

1. **Specific Objective** 1: Key state (governance and security) actors are better equipped to prevent and address violent extremism and apply gender responsive/transformative approaches to their PCVE strategies and actions.

   Outputs:
   1.1 National strategy on preventing and responding to violent extremism is reviewed (to include women's on PCVE and address the discriminatory power dynamics and social normsrole on PCVE) and implemented by the National Counter Terrorism Centre by connecting and coordinating the national and regional network.

   1.2 Enhanced PCVE skills and resources of key national and local authorities, as well as those of the frontline workers cooperating with them, are strengthened (particularly as regards early warning as well as preventive and early actions that are gender responsive/transformative.)

   1.3Support to the creation of formal and informal structures and mechanisms of information and dialogue between key state and non-state actors (including women and youth in all their diversity) at national and regional level.

2. **Specific Objective** 2: The resilience of the communities and women and men in all their diversity at risk of suffering from (or being engaged in) violent extremism is strengthened.

   Outputs:
   2.1 Community focused and driven initiatives for the prevention of violent extremism in beneficiary counties are supported (including promoting positive masculinity and support for gender equality including challenging harmful gender norms)

   2.2 Community level civil society organisations (including youth and women's organisations) and local (including religious and local leaders) actors have increased capacity to be partners in the prevention of violent extremism.

   2.3 Young women and men strengthen their resilience for peace and against violent extremism.

3. **Specific Objective** 3: The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure, gender responsive and peaceful cyberspace.

   Outputs:

   3.1 Adoption and implementation of a coherent, holistic, gender responsive, strategic and actionable national approach to cyber resilience is facilitated

3.2 National operational capacities to adequately prevent, respond to, and recover from cyber-attacks and/or accidental failures are improved

3.3 Trust of users, organisations and companies in the use of the cyberspace is enhanced (from a human rights and gender perspectives).

3.2 Indicative Activities

Activities relating to Output 1.1

- Develop and review policies, legal frameworks, and regulations to address emerging trends in radicalization and violent extremism using gender responsive approaches
- Support devolved units/structures in the implementation of County Action Plan (including gender units/expertise)
- Strengthen the capacity the National Counter Terrorism Centre to maintain high levels of effectiveness in its fusion/ coordination mandate to ensure the implementation of the National Strategy on PCVE, including its gender components

Activities relating to Output 1.2

- Train key national and local actors in the implementation of new policies and frameworks to be developed under output 1.1, with an emphasis on gender responsive/transformative approaches.
- Improve technical strategic communications skills of relevant actors through a gender responsive/transformative approach, in support of the StratCom strategy.
- Train frontline workers in identifying and responding to radicalization and violent extremism, with an emphasis on gender equality and women's and girl's empowerment.
- Conduct gender responsive/transformative research including surveys, risk/threat assessments, and radicalisation indices to guide interventions, inform policies and produce early warning opportunities

Activities related to Output 1.3

- Annual forum on PCVE is organised at national and local level with representatives from the state, the local communities and CSOs (including universities and women organisations).
- Develop a response mechanism and support the development of a Violent Extremist Offenders framework to reduce recidivism and facilitate successful reintegration of violent extremists
- Support the implementation of the StratComm strategy to protect communities against extremists' propaganda.

Activities relating to Output 2.1

- Provide small grants to community-level, grassroots initiatives (including those led by women) that address the local drivers and triggers of violent extremism (such as mistrust between communities and the security and policy forces or local grievances).
- Awareness raising on PVE issues, including human rights, gender equality and women's rights and PVE, in communities through radio and TV stations.
- Women's and Youth Economic empowerment: income generating activities, vocational /entrepreneurs/life skills training small business seed funding; linking communities with markets and employment opportunities

Activities relating to Output 2.2

- Training (including human rights and gender equality and women's rights) for journalist and creators of online content on alternative and peaceful narratives.
- Support the creation of youth associations (including women's youth associations as well as gender balance in the mixed ones) and platforms for civic engagement in the communities at risk

Activities relating to Output 2.3

- Support school and family reintegration for disconnected youth, economic empowerment through skills training and job placements following their social engagement in PVE activities.
- Train young people, both women and men, formally and informally to develop critical skills to identify and peacefully react to violent extremist content online
- Empowering youth living in the most vulnerable situations (via the County Engagements forum, sports activities such as football etc.) the civic engagement to address local sources of conflict (including discriminatory power dynamics and rigid gender norms and structures)

Activities related to output 3.1

- Improvement of regulatory guarantees for CIIP drafted/updated with the support of the action
- Support the creation of a crisis management mechanism
- Assistance in connecting organisations to the monitoring and SOC infrastructure
- Support to the upgrade of the KE CIRT to National KE CIRT

Activities related to output 3.2

- Draft and implement text of risk framework/guidelines
- Improving parameters for KE-CIRT for organisational structure, human resources, tools and processes
- Assistance in connecting organisations to the monitoring and SOC infrastructure
- Develop a cybersecurity basic education curriculum

Activities related to output 3.3

- Awareness and cyber hygiene practices of individual users (e.g. employees, citizens, students) are improved
- Provisions promoting cyber hygiene and technical standards in line with existing international best practices (i.e. ICT security standards and cryptographic controls, procurement standards for ICT, etc.) are introduced in laws, regulations and government tenders
- Cyber awareness and incorporation of gender responsive cyber hygiene technical standards in line with existing international best practices are rolled out in governmental services

The commitment of the EU's contribution to the Team Europe Initiative foreseen under this action plan will be complemented by other contributions from Team Europe partners. It is subject to the formal confirmation of each respective partners' meaningful contribution as early as possible. In the event that the TEIs and/or these contributions do not materialise the EU action may continue outside a TEI framework.

3.3 Mainstreaming

Environmental Protection & Climate Change

At this stage the EIA (Environmental Impact Assessment) screening undertaken by the EUD points to the project having little or no impact on the environment or on climate change given the nature of the proposed

activities. This action will support and promote the adoption of climate smart technologies where applicable.

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. Given that, the desired impact of this action will not be realised without systematically applying gender mainstreaming to all of its activities: policy development, capacity building and awareness raising activities which will put a particular emphasis on the active participation of and inputs from women, in all their diversity. Therefore, particular attention will be paid to those patriarchal societal structures (gender norms, systemic gender-based violence and intersectionality – multiple inequalities and discriminations) that are part of the dynamics that violent extremism poses in the particular context of Kenya.

The action will contribute to the Gender Action Plan III (GAP III)[6], especially to the thematic objective "Addressing the challenges and harnessing the opportunities offered by the digital transformation".

Human Rights

The Action is aligned with the EU Action Plan on Human Rights and Democracy 2020-2024[7], on harnessing opportunities and addressing challenges of digital technologies. The activities are underpinned by a human rights-based approach, but also specifically work towards the realisation of specific human rights. The intervention contributes to the 2030 Agenda which is anchored in international human rights namely towards SDG 16 (peace, justice and strong institutions). The action will implement the five working principles in all phases: i) respect to all human rights, ii) participation, iii) non-discrimination iv) transparency and v) accountability.

A clear human-rights-based approach will be incorporated throughout the different stages of the project cycle (project design/formulation; monitoring of implementation; evaluation) on the basis of the operational guidance developed to this end by the European Commission.[8] Any potential flow-on risk on the respect of human rights should be constantly monitored and mitigating measures need to be foreseen, including in relation to the human rights record of security and intelligence actors, issues of gender responsiveness and possible lack of independence of the criminal justice system. Also, Pillar IV of the UN Global Counterterrorism Strategy reaffirms that the promotion and protection of human rights is essential to all measures against terrorism. It also recognises that counterterrorism measures and the protection of human rights are not conflicting goals, but rather complimentary and mutually reinforcing.

Disability

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D1. This implies that in line with the EU strategy for the rights of persons with disabilities, this action will strive to ensure systematic inclusion.

Reduction of inequalities

[6] (https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2184)

[7] JOIN (2020) 5 final of 25.03.2020

[8] (https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperationactions-addressing-terrorism-organised_en).

Kenya is one of the countries in Africa that has high levels of inequality. However, the income Gini coefficient for Kenya is relatively low compared to other African economies that are characterised by high levels of income inequality, such as South Africa and Botswana, but it is still high relative to many countries in the region. Nevertheless, in East Africa, Kenya has the highest inequality indicators compared to her neighbours, Uganda, Tanzania and Ethiopia. The action aims to reduce vulnerabilities and prevent risks through actions that tackles inequality and marginalisation.

Democracy

The action is aligned with the EU Action Plan on Human Rights and Democracy 2020-2024[9], on the fair administration of justice and democratic institutions, while supporting the implementation of the Human Rights and Democracy country strategy 2021-2024. CSOs are a core component of the action in line with the Civil Society Roadmap.

Conflict sensitivity, peace and resilience

The re-emergence of ethnic divides and related discrimination and marginalisation are key challenges to the stability of the country. In addition, the porous borders with neighbouring countries pose challenges for cross-border organised crime, trafficking in human beings, smuggling of migrants and terrorism and the proliferation of violent extremism behaviour especially among youth. A relatively weak governance structure of operation on cybersecurity renders Kenya poorly prepared to complex cybersecurity attacks. Mitigation measures include addressing drivers of conflict, countering terrorism and violent extremism and direct support to secure the resilience of the cyberspace. Conflict sensitivity will be a key feature, based on the findings and recommendations of the 2022 Conflict Screening Assessment. Gender mainstreaming will be an important feature of the first component on CT-PCVE, in particular by integrating the Women, Peace and Security Agenda.

Disaster Risk Reduction

With conflict and disaster risks being the result of similar underlying causes and multiple vulnerabilities, this action tackles drivers of conflict and disasters such as the risks posed by marginalisation and poverty. However, focusing on leaving no one behind, by seeking at including the vulnerable categories (including IDPs and refugees) in the conflict prevention directly contributes to reducing the disaster risks. Furthermore, access to digital services in a cyber-secure environment directly contributes to improving the safety of the digital use and has a direct impact on reducing the risks posed by cyber-attacks to the vital infrastructure.

3.4 Risks and Lessons Learnt

Category	**Risks**	**Likelihood (High/ Medium/ Low)**	**Impact (High/ Medium/ Low)**	**Mitigating measures**
Communication and Information	Disinformation and misinformation on	**Medium**	**High**	The NCTC has a communication strategy to

[9] JOIN (2020) 5 final of 25.03.2020.

	the implementation of the action.			counter such disinformation and misinformation.
Local acceptance	Doing more harm than good in the area of P/CVE.	**Medium**	**High**	Comprehensive and rigorous needs assessment will be carried out prior to commencing any work. The recipients will be carefully selected and supported in designing and developing strong programmes.
Conflict	Politicization of the P/CVE programmes by some stakeholders which may derail the programme	**Low**	**Medium**	The NCTC will engage all stakeholders to build consensus that violent extremism is a societal problem that affects us all.
Security risks	Security risks for the grantees and programme participants, including women and girls involved in P/CVE activities	**Low**	**High**	Extreme care and due diligence on external communications and safeguard the anonymity and safety of grantees and programme participants. Guidance will be sought from local CSOs and women on how to label their CVE activities and on necessary security measures.
Discriminatory societal norms and power dynamics	Lack of gender awareness, gender sensitivity, gender understanding increase/perpetuate existing gender inequality and discriminatory social norms and power dynamics	**Medium**	**High**	Include gender analysis and at least sex/age and disability desegregated data. Make sure there is an inclusive participation and gender balance among interventions' rights holders
Political risks	Support for change at the political and policy level	**Low**	**Medium**	Capacity building on the importance of aligning the cybersecurity policy with the international standards is embedded in the cybersecurity programme.
Funding risks	Adequate level of financing is sustained in both	**Medium**	**High**	Importance of adequate funding from the government is included in the strategic dialogue with Kenya. This will be further mitigated by

	PCVE as well as cybersecurity			ensuring that adequate benchmarking with similar institutions in Europe, which will look at both operational as well as financial means.

Lessons Learnt:

The action draws critical lessons from the 2018 – 2022 Kenya – EU partnership on the implementation of the NSCVE, key being identification and prioritisation of the most vulnerable and development of community led solutions to violent extremism. This action is therefore instrumental in strengthening the long-standing Kenya-EU partnership on security and development. In implementing the National Strategy on Countering Violent extremism, through the first phase of EU-NCTC Support to the implementation of the Countering violent Extremism strategy, several lessons have emerged: (1) terrorism and violent extremism are dynamic challenges playing out in a fluid environment therefore the need to be context specific and agile in responses, (2) it is critical to identify and prioritise the most vulnerable hence support provided to the grassroots and community level is essential, (3) target primarily identified hotspots where there is need to build resilience among communities that would in future be targeted by radicalisers, (4) initiatives need to be devolved to local levels where communities identify their own priorities and align them to the national strategy allowing for bottom up diagnosis and action, (5) there is need to adopt a coherent framework to monitor and evaluate interventions operating in the same field, (6) it is imperative to have adequate resources at both national and local levels, (7) the effective participation of women, youth and minorities (8) empowering victims of terrorism (9) mainstreaming PCVE in all relevant government activities is key in the sustainability of the program and (10) regional and international partnerships are integral in bringing international best practice and mobilising resources for effective implementation. The achievements of the current NCTC partnership gave strategic impetus to the development of County Action Plans and their implementation, which are community-led and owned initiatives to prevent violent extremism at the local level. The support was vital in assisting the National Counter Terrorism Centre to adapt and respond to the dynamic and mutating nature of the threat. The partnership facilitated the development of innovative, sustainable, community-based solutions that have been impactful and transformative in building resilience and addressing the drivers of radicalisation. Furthermore, the partnership has increased the technical capacity and expertise of the national government and the local significantly in countering violent extremism.

Main lessons learned from previous EU programming on P/CVE call for this to be evidence-based, tailored according to the local context, and adopting a multi-disciplinary approach. These aspects have been taken into account in the design of the components. In addition, the proposed components seek to develop further knowledge throughout the implementation to facilitate learning in this complex and challenging domain, and to ensure that steps taken are coherent with the other endeavours and interventions. The proposed component builds on the good practices and lessons learned identified during past work in focus communities with EU support among others.

3.5 The Intervention Logic

Specific Objective 1

By supporting the Government of Kenya to progressively transform its approach to PCVE in delivering a more transparent, accountable, and integrated approach to violent extremism the overall security in the country will improve. As a result, the risks, and implications of violent extremists' activities on national and regional security and stability will be reduced. The action's intervention logic is based on two main elements: (1) if the action strengthens the National Counter Terrorism Centre in delivering its mandate, it will improve the approaches to violent extremism and shrink the pool of individuals at risk of recruitment into radicalised groups; and (2) if the action assists the National Counter Terrorism Centre in addressing underlying factors and promoting a whole of society approach, Kenyan communities shall emphatically and continuously reject violent extremists' ideologies and aims.

Specific Objective 2

If communities' resilience to violent extremism will be increased, all this will result in a reduction of the terrorist threat and in levels of extremism-related violence and in a positive, sustainable contribution to increased stability in the areas in which the activities have been implemented.

Specific Objective 3

If the resilience of the cybersecurity ecosystem will be strengthened this will contribute to increase state and societal capacity to manage cyber incidents and crises in a time, effective and efficient manner. With Kenya increasingly reliant on the use of ICT to optimise various critical and non-critical infrastructure, it is paramount to identify vulnerabilities in the inter-linked networks and information systems that could be exploited for political or financial gains.

3.6 Logical Framework Matrix

This indicative logframe constitutes the basis for the monitoring, reporting and evaluation of the intervention.
Based on this logframe matrix, a more detailed logframe (or several) may be developed at contracting stage. In case baselines and targets are not available for the action, they should be informed for each indicator at signature of the contract(s) linked to this AD, or in the first progress report at the latest. New columns may be added to set intermediary targets (milestones) for the Output and Outcome indicators whenever it is relevant.

- At inception, the first progress report should include the complete logframe (e.g. including baselines/targets).
- Progress reports should provide an updated logframe with current values for each indicator.
- The final report should enclose the logframe with baseline and final values for each indicator.

The indicative logical framework matrix may evolve during the lifetime of the action depending on the different implementation modalities of this action.
The activities, the expected Outputs and related indicators, targets and baselines included in the logframe matrix may be updated during the implementation of the action, no amendment being required to the Financing Decision.

Results	**Results chain (@): Main expected results (maximum 10)**	**Indicators (@): (at least one indicator per expected result)**	**Baselines (values and years)**	**Targets (values and years)**	**Sources of data**	**Assumptions**
Impact	To reduce incidents of violent extremism and cybersecurity attacks in Kenya	1. The Global Terrorism Index (GTI) 2. Number of violent extremism incidents in Kenya across the duration of the project 3.Number of cyber security incidents in Kenya across the duration of the project	1. 2022-6.17 2. 2023 – TBD in project baselines 3. 2024- TBD in project baselines	1. 2027- 20%decrease 2. 2027-20% decrease 3. 2027- 20%	1. Global Terrorism Index 2. Project and country reports 3. Project and country reports	N/A
Outcome 1	1: Key state (governance and security) actors are better equipped to prevent and address violent extremism and apply gender responsive / transformative approaches to their PCVE strategies and actions.	1.1 Number of gender responsive/transformative County PCVE Plans of Actions supported and implemented 1.2 Number of tools, modules and SOPs developed and reviewed (from a human rights and gender responsive/transformative approach) 1.3 Number of policies, legal frameworks and regulations developed and reviewed (from a	1.1 2023 -0 1.2 2023 -0 1.3 2023-0	1.1 2027-at least 10 CAPs supported 1.2 2027-TBD 1.3 2027-TBD	Project report Country Specialised Reports	The underlying assumption is that the government remains committed to implementing and further adapting the national strategy on countering violent extremism

		human rights and gender responsive/transformative approach)				
Outcome 2	The resilience of the communities and women and men in all their diversity at risk of suffering from (or being engaged in) violent extremism is strengthened.	2.1 Changes in attitudes (including gender discriminatory norms, attitudes and beliefs) towards government and violent groups, measured by perception surveys before, during and after a project. 2.2 Percentage of 'at-risk' individuals with gainful employment (disaggregated at least by sex, age, disability and minority group if possible) 2.3 Changes in the percentage of targeted women and men, in all their diversity, who feel less marginalised.	2.1 2024 –to be established by baseline studies 2.2 2024- to be established by baseline studies 2.3 2024- to be established by baseline studies	2.1 2027-TBD 2.2 2027-50% of individuals disaggregated by at least by sex, age, disability and minority group if possible 2.3 2027 – 80% of individuals targeted	2.1 Project surveys 2.2 Project reports 2.3 Project reports	It is assumed that the actions will be able to operate in the areas where most "at risk" individuals are. In addition, it is assumed that the government will continue to allow the PCVE actions to take place in these areas.
Outcome 3	The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure, gender responsive and peaceful cyberspace.	Country position in the ITU Global Cybersecurity and Cyber wellness Index (sources Global Cybersecurity and cyber wellness Index. Network readiness index Freedom on the net report)	2023 – 41.56	2027-3 positions increased	ITU Global Cybersecurity wellness index	The underlying assumption is that the government remains committed to implementing and further adapting the national strategy on cybersecurity and it will allocate sufficient funds to it
Output 1 **relating to Outcome 1**	1.1 National strategy on preventing and responding to violent extremism is (to include women's role on PCVE and address the discriminatory power dynamics and social norms)reviewed and implemented by the National Counter Terrorism Centre by catalysing, connecting and coordinating the national and regional network.	1.1.1 NSCVE reviewed and launched (including a gender responsive perspective)	1.1.1 2023-0	1.1.1 2027-1	National reports Country Specialised Reports	

Output 2 **relating to Outcome 1**	1.2 Enhanced PCVE skills and resources of key national and local authorities, as well as those of the frontline workers cooperating with them, are strengthened (particularly as regards early warning, preventive and early actions that are gender responsive/transformative. etc.)	1.2.1 Number of frontline workers trained on PCVE (disaggregated at least by sex and age) 1.2.2 Number of individuals directly reached through the disengagement program (disaggregated at least by sex gender, age and disability, migratory status)	1.2.1 Project reports and baselines 1.2.2 2023-0	1.2.1 2027- 20%of the eligible workforce trained disaggregated at least by sex and age 1.2.2 2027-TBD	Project report Country Specialised Reports	The underlying assumption is that the government remains committed to implementing and further adapting the national strategy on countering violent extremism
Output 3 **Relating to Outcome 1**	1.3 Support to the creation of formal and informal structures and mechanisms of information and dialogue between key state and non-state actors (including women and youth in all their diversity) at national and regional level.	1.3.1 Number of regular stakeholders' engagements at county level between state and non-state actors (disaggregated by age and sex) 1.3.2 Number of Inter and Intra faith dialogues held	1.3.1 2023 -0 1.3.2- 0	1.3.1 3/year until 2027 1.3.2 2/year until 2027	Project reports	
Output 1 **relating to Outcome 2**	2.1 Community focused and driven initiatives for the prevention of violent extremism in beneficiary countries are supported (including promoting positive masculinity and support for gender equality including challenging harmful gender norms).	2.1.1 Number of religious and community leaders supported for the prevention of violent extremism (disaggregated by sex and age) 2.1.2 Number of gender responsive/transformative tailored made initiatives designed? Implemented? in the hot spots of violent extremism	2.1.1 2024- 0 2.1.2 2024- 0	2.1.1 TBD in each sub grant - #disaggregated by age and sex 2.1.2 TBD in each sub-grant #disaggregated by age and sex	Project reports	
Output 2 **relating to Outcome 2**	2.2 Community level civil society organisations (including youth and women's organisations) and local actors (including religious and local leaders) have increased capacity to be partners in the prevention of violent extremism.	2.2.1 Number of civil society organisation at local level supported (including number of youth and women's rights organisations) 2.2.2. Number of initiatives launched by the beneficiary civil society organisations thanks to the support of the EU (including those of youth and women's rights organisations)	Baseline done in 2024	2.2.1 2027 – TBD in each sub grant	Project reports	

Output 3 Relating to Outcome 2	2.3 Awareness and knowledge of good practices in P/CVE and women, peace and security is increased among the youth in the most vulnerable situations.	2.2.3 Number of stakeholder engagement (disaggregated by sex and age)	2.2.3 2024-0	2.2.3 2027 – TBD in each sub grant	Project reports	
Output 1 Relating to Outcome 3	3.1 Adoption and implementation of a coherent, holistic, gender responsive, strategic and actionable national approach to cyber resilience is facilitated	3.1.1 Status of risk management framework/guidelines for the national authorities designed/updated with the support of the Action 3.1.2 Number of decision-makers trained by the Action on the implementation of national cybersecurity strategies (disaggregated by sex and age)	3.1.1 2024-0 3.1.2 2024-0	3.1.1-TBD 3.1.2 2027-TBD	Action's reports/database of mentored staff (disaggregate by age and sex)	Stakeholders have a clear understanding of their roles and responsibilities Good cooperation among ministries and agencies and acceptance of change
Output 2 Relating to outcome 3	3.2 National operational capacities to adequately prevent, respond to, and recover from cyber-attacks and/or accidental failures are improved	3.2.1 Status of policy provisions and/or regulations defining the responsibilities and resources of institutions competent for prevention, protection and recovery from cyber-attacks and/or accidental failure 3.2.2 The national CERT has established parameters for organisational structure	3.2.1 2024- TBD in baseline 3.2.2 2024 -0	3.2.1 2027- implemented/adopted 3.2.2 2027 -1	National records Text of regulatory framework for CIIP Text of the guidelines on cyber crisis management National CERT annual activity report	It assumes the government will continue to put significant emphasis on the cybersecurity strategy and its implementation by also allocating sufficient resources
Output 3 Relating to outcome 3	3.3 Trust of users, organisations and companies in the use of the cyberspace is enhanced (from a human rights and gender perspectives)	3.3.1. Number of MoUs between key private sector entities (CII operators, vendors) and government bodies 3.3.2 Number of staff trained with the support of the Action on cyber hygiene practices and technical standards (disaggregated at least by sex, age and disability)	3.3.1 2024 – TBD 3.3.2 2024 -0	3.3.1 -2027 TBD fort the CII operators 3.3.2 – at least 1/3 of the core staff identified by the government trained	National records	

4 IMPLEMENTATION ARRANGEMENTS

4.1 Financing Agreement

In order to implement this action, it is not envisaged to conclude a financing agreement with the partner country.

4.2 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 adoption by the Commission of this Financing Decision.

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.

4.3 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[10].

4.3.1 Direct Management (Grants)

4.3.1.1 Outcome– Specific Objective 1

Grants: (direct management)

(a) Purpose of the grant(s)

The purpose of the grant to be awarded under Specific Objective 1 is to strengthen the capacity of the National Counter Terrorism Centre to implement the National Strategy on Countering Violent Extremism.

(b) Type of applicants targeted

The grants are open to public bodies working on preventing violent extremism and counter terrorism at national level.

4.3.1.2 Outcome Specific Objective 2

Grants: (direct management)

(a) Purpose of the grant(s)

The purpose of the grants to be awarded under Specific Objective 2 is to work with the local communities and Civil Society Organisations and local communities to develop and implement interventions that have a demonstrable impact on the threat posed by radicalisation and recruitment to terrorism.

(b) Type of applicants targeted

The grants will be open for funding to NGOs operating in the areas prone to violent extremism in Kenya.

4.3.2 Indirect Management with an entrusted entity

A part of this action may be implemented in indirect management with an entrusted entity, which will be selected by the Commission's services using the following criteria: have knowledge, expertise and mandate to implement operations in cybersecurity. The organisation will need to have experience in rolling out significant cyber security

[10] www.sanctionsmap.eu. 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.

projects in Africa while experience of working in Kenya will be a distinct advantage. The entrusted entity will need to have sufficient presence in Kenya or the capacity to deploy permanent presence for the implementation of the action. The entrusted entity will need to demonstrate capacity of implementation of European Frameworks on cybersecurity and have expertise and knowledge of the European policy on cyber security.

The implementation by this entity entails the part of the action related to the significant objective 3, *The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure and peaceful cyberspace.*

4.3.3 Changes from indirect to direct management mode (and vice versa) due to exceptional circumstances (one alternative second option)

In case of the indirect management under the point 4.3.2 fails, this part of the action under Specific Objective 3 - The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure and peaceful cyberspace - could be implemented by a twinning grant (direct management). The twinning Fiche will align its objectives/results with the ones identified for Component 3 - *The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure and peaceful cyberspace.*

The part of the action under the budgetary envelope reserved for grants may, partially or totally be implemented in indirect management with an entity, which will be selected by the Commission's services using the following criteria:

- experience of implementing actions on prevention of violent extremism and mentorship programmes for youth in Kenya,
- experience in running psycho-social support programmes in Kenya for vulnerable population at risk of violent extremism.
- extensive presence in Kenya on implementing national policies on countering violent extremism.

4.4. 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).

4.5. Indicative Budget

Indicative Budget components[11]	**EU contribution (amount in EUR) Year 2023**	**EU contribution (amount in EUR) Year 2024**
Implementation modalities – cf. section 4.3.		
Specific Objective 1: Key state (governance and security), media and non-state actors at national and community levels prevent and address violent extremism	**0**	**5 000 000**
Grants (direct management) – cf. section 4.3.1	N/A	5 000 000

[11] N.B: The final text on audit/verification depends on the outcome of ongoing discussions on pooling of funding in (one or a limited number of) Decision(s) and the subsequent financial management, i.e. for the conclusion of audit contracts and payments.

Specific Objective 2: Individuals identified as at risk of violent extremism demonstrate more resilient attitudes and behaviours	**0**	**2 000 000**
Grants (direct management) – cf. section 4.3.1	N/A	2 000 000
Specific Objective 3: The resilience of the cybersecurity ecosystem of Kenya is strengthened and ensures that citizens enjoy an open, free, secure and peaceful cyberspace.	**0**	**3 000 000**
Indirect management with an entrusted entity- cf. section 4.3.2		3 000 000
Grants –total envelope under section 4.3.1		7 000 000
Evaluation – cf. section 5.2 **Audit** – cf. section 5.3	N/A	may be covered by another Decision[12]
Totals	**0**	**10 000 000**

4.6 Organisational Set-up and Responsibilities

Specific Objective 1

The governance mechanism of the action involves a Programme Board composed of representatives from the Centre and the EU. The permanent members will jointly decide to invite other entities to join the board as observers. The Board will ensure strategic direction of activities, and as such, will oversee, pilot, and suggest readjustments of the action, if need be, as well as act as a forum for discussing and agreeing on wider issues. The Board will meet periodically but no less than twice a year to allow adapting and adjusting in real time. The Board will be supported by a technical committee formed from members of the NCTC, The National Treasury, Ministry of Interior and the EU as observer. The Technical Committee will periodically inform the progress on milestones.

Specific Objective 2

The governance mechanism of the action will be structured according to the selected grants. It will nevertheless include members of the National Counter Terrorism Centre, the Grantees, and members of the County Engagements Forum, County Governments and the EU as observer.

Specific Objective 3

The project will be steered by a steering committee located within the National Computer and Cybercrimes Coordination Committee (NC4) and its secretariat. To de-conflict and align interventions, the steering committee will include the ongoing regional programme supported by the European Union under the Horn of Africa Initiative on cybersecurity, or other complementary programmes.

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 and may sign or enter into joint declarations or statements, for the purpose of enhancing the visibility of the EU and its contribution to this action and ensuring effective coordination.

5 PERFORMANCE MEASUREMENT

5.1 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

[12] Where the action is not covered by a financing agreement (see section 4.1), but 'will be covered by another Decision' as it is unlikely that evaluation and audit contracts on this action would be concluded within N+1. These contracts have to be authorised by another Financing Decision.

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 results (Outputs and direct Outcomes) 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). All monitoring and reporting shall assess how the action is considering the principle of gender equality, human rights-based approach and rights of persons with disabilities including inclusion and diversity. Indicators shall be disaggregated at least by sex and age, and disability if possible.

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).

Roles and responsibilities for data collection, analysis and monitoring:

Component 1 and 3: Data collection for baselines will be included in each of the project intervention. The responsibility for accurate and timely collection lies with the selected implementing partners. The indicators at the national level will be established, monitored and reported on from the governance structures embedded in the projects, which include the relevant government bodies. Each of the selected implementing partner will be responsible for collecting and monitoring the data collection and will include adequate finance related to it.

Component 2 will be designed in participatory manner with the CSOs embedded in the local structures i.e. County Engagements Forum. Monitoring and Evaluation as well as collection of data will be done at the sub-grantees level, while aggregation and reporting of results will be done by GCERF.

5.2 Evaluation

Having regard to the nature of the action, a mid-term evaluation(s) may be carried out for this action or its components via independent consultants contracted by the Commission. It will be carried out for problem solving and learning purposes, in particular with respect to the selection of the grantees for component 2 and to assess the level of implementation of component 3 which is a new field of action for the European Union in Kenya. Evaluation shall also assess to what extent the action is taking into account the human rights-based approach as well as how it contributes to gender equality and women's empowerment and disability inclusion. Expertise on human rights, disability and gender equality will be ensured in the evaluation teams

The Commission shall inform the implementing partner at least one month in advance of the dates envisaged for the evaluation 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 may be shared with the partners and other key stakeholders following the best practice of evaluation dissemination[13]. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, apply the necessary adjustments.

The financing of the evaluation may be covered by another measure constituting a Financing Decision.

5.3 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.

[13] See best practice of evaluation dissemination

6 STRATEGIC COMMUNICATION AND PUBLIC DIPLOMACY

The 2021-2027 programming cycle will adopt a new approach to pooling, programming and deploying strategic communication and public diplomacy resources.

In line with the 2022 "Communicating and Raising EU Visibility: Guidance for External Actions", it will remain a contractual obligation for all entities implementing EU-funded external actions 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. This obligation will continue to apply equally, regardless of whether the actions concerned are implemented by the Commission, partner countries, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU member states.

However, action documents for specific sector programmes are in principle no longer required to include a provision for communication and visibility actions promoting the programmes concerned. These resources will instead be consolidated in Cooperation Facilities established by support measure action documents, allowing Delegations to plan and execute multiannual strategic communication and public diplomacy actions with sufficient critical mass to be effective on a national scale.

- # Appendix 1 REPORTING IN OPSYS

A Primary Intervention (project/programme) is a coherent set of activities and results structured in a logical framework aiming at delivering development change or progress. Identifying the level of the primary intervention will allow for:

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

Primary Interventions are identified during the design of each action by the responsible service (Delegation or Headquarters operational Unit).
The level of the Primary Intervention chosen can be modified (directly in OPSYS) and the modification does not constitute an amendment of the action document.

The intervention level for the present Action identifies as (tick one of the 4 following options);

Action level (i.e. Budget Support, blending)		
☐	Single action	Present action: all contracts in the present action
Group of actions level (i.e. top-up cases, different phases of a single programme)		
☐	Group of actions	Actions reference (CRIS#/OPSYS#): <Present action> <Other action(s)>
Contract level		
x	Single Contract 1	Grant
x	Single Contract 2	Grant
x	Single Contract 3	Contribution agreement
Group of contracts level (i.e. series of programme estimates, cases in which an Action includes for example four contracts and two of them, a technical assistance contract and a contribution agreement, aim at the same objectives and complement each other)		
☐	Group of contracts 1	<foreseen individual legal commitment (or contract) 1> <foreseen individual legal commitment (or contract) 2> <foreseen individual legal commitment (or contract) #>