EN

ANNEX 2

of the Commission Decision on the Annual Action Programme 2017 - part II - in favour of the Caribbean Region to be financed from the 11th European Development Fund

Action Document for Capacity Development for CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime

| INFORMATION FOR POTENTIAL GRANT APPLICANTS

WORK PROGRAMME FOR GRANTS

This document constitutes the work programme for grants in the sense of Article 128(1) of the Financial Regulation (Regulation (EU, Euratom) No 966/2012), applicable to the EDF by virtue of Article 37 of the Regulation (EU) No 323/2015 in the following sections concerning grants awarded directly without a call for proposals: 5.4 |

<table>
<thead>
<tr>
<th>1. Title/basic act/ CRIS number</th>
<th>Capacity Development for CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime CRIS number: FED/2017/040-086 financed under the 11th European Development Fund</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Zone benefiting from the action/location</td>
<td>CARIFORUM Member States; Antigua &amp; Barbuda, The Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Lucia, Saint Kitts &amp; Nevis, St. Vincent &amp; the Grenadines, Suriname, Trinidad and Tobago and the Dominican Republic. The action shall be carried out at the following location: Two project teams which will be based in Trinidad and Tobago, and one project team location to be determined (implementing partner to be selected via PAGoDA 2 Delegation Agreement).</td>
</tr>
<tr>
<td>3. Programming document</td>
<td>Caribbean Regional Indicative Programme 11th European Development Fund</td>
</tr>
<tr>
<td>4. Sector of concentration/thematic area</td>
<td>Focal area 3 – Crime and Security DEV. Aid: YES</td>
</tr>
<tr>
<td>5. Amounts concerned</td>
<td>Total estimated cost: EUR 8 450 000 Total amount of EDF contribution EUR 8 450 000</td>
</tr>
<tr>
<td>6. Aid modality(ies) and implementation modality(ies)</td>
<td>Project Modality Component A: Direct management – Grant, direct award to CFATF Component B: Pillar Assessed Grant Agreement</td>
</tr>
</tbody>
</table>
**Component C: Direct management – Grant, direct award to CARICOM/IMPACS**

Direct management – Procurement of services

### 7 a) DAC code(s)

- 15110 – Public sector policy and administrative management
- 15111 – Public finance management
- 15220 – Security system management and reform

### b) Main Delivery Channel

- 10000 – Public sector institutions

### 8. Markers (from CRIS DAC form)

<table>
<thead>
<tr>
<th>General policy objective</th>
<th>Not targeted</th>
<th>Significant objective</th>
<th>Main objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation, development/good governance</td>
<td>☐</td>
<td>☐</td>
<td>x</td>
</tr>
<tr>
<td>Aid to environment</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Gender equality (including Women In Development)</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Trade Development</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Reproductive, Maternal, Newborn and child health</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**RIO Convention markers**

<table>
<thead>
<tr>
<th>Biological diversity</th>
<th>Not targeted</th>
<th>Significant objective</th>
<th>Main objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combat desertification</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Climate change mitigation</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Climate change adaptation</td>
<td>x</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

### 9. Global Public Goods and Challenges (GPGC) thematic flagships

- N/A

### 10. Sustainable Development Goals (SDGs)

- SDG 16 "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels” and in particular targets 16.4, 16.6 and 16a.

**Summary**

The overall objective is to contribute to improvement of safety and security in the CARIFORUM region.

The specific objectives are to increase compliance in the CARIFORUM region with international norms on money laundering, countering the financing of terrorism and other financial crimes while also improving the capacity of CARIFORUM Member States to deal with the issue of cybercrime.

Supporting Financial Compliance is an explicit objective in the Caribbean Regional Indicative Programme (CRIP) under Result 3.1. Financial Compliance is also listed as an area of specific concern in the Joint Caribbean-EU Strategy and is fully in line with the CARICOM Crime and Security Strategy. Combating money laundering is also listed as cooperation area of importance in the EU Strategy on Citizen Security in Central America and the Caribbean. Cybercrime is deemed as an immediate and significant threat in the CARICOM Crime and Security strategy and in the CARICOM Strategic Plan for the Caribbean Community 2015-2019. Cybercrime is also included in the Joint Caribbean-EU Strategy as an area of specific concern to both regions.

Component A – Implementation of the Mutual Evaluation Programme
This component will support countries to carry out and follow up on the Financial Action Task Force on Money Laundering (FATF) Fourth Round of Mutual Evaluation Missions, which will include support in the form of financial support (50% of the cost of the missions) and training packages.

Component B – National Risk Assessments and National Action Plans
This component will support CARIFORUM Member States in carrying out National Risk Assessments as well as support to the design and implementation of National Action Plans. Additionally support will be given to Work Plans that have been developed as result of National Risk Assessments.

Component C – Asset Recovery and Cybercrime
This component will focus on capacity building for CARIFORUM Member States on two separate issues with similar stakeholders; asset recovery and cybercrime. As the capacity building for these two activities will be coordinated by the same implementing agency (CARICOM/IMPACS) they are included within one component.

There are important interlinkages between thee three components and therefore the implementing partners will coordinate closely to ensure complementarity, avoid duplication and build synergies.

1. CONTEXT

1.1 Regional and thematic context
Organised and transnational crime poses a threat to Caribbean governments, economies and citizens. While criminals can easily operate across borders, state prevention of crime transcending national borders is more complicated. To combat criminal activities such as cybercrime, money laundering and the financing of terrorism there is a need to build the operational capacity of state institutions. Preventing these crimes necessitates strong state systems as well as networks for collaboration and exchange of information. International initiatives, such as the Financial Action Task Force on Money Laundering (FATF) and the Council of Europe’s Convention on Cyber Crime (the Budapest Convention), provide guidelines and information on how to strengthen state capacity to counter organised and transnational crime.

This project aims to support the Caribbean countries in aligning their financial systems and state institutional structures with such international standards and to promote their engagement and collaboration regionally and internationally.\(^1\)

Component A – Implementation of the Mutual Evaluation Programme
Component B – National Risk Assessments and National Action Plans
Financing of terrorism and money laundering – while differing in several aspects – exploit similar vulnerabilities in national and international financial systems. The Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body set up by the G7 group in 1989 with the objective to set policy and standards to combat money laundering as well as the financing of terrorism. FATF has produced a comprehensive set of international standards which are accepted internationally as the global policy guidelines on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). The 2012 FATF standards consist of core recommendations relating to AML/CFT with additional guidance on how countries can comply with these standards.

\(^1\) The programme is supporting the region to comply with international guidelines (FATF and the Budapest Convention) – the compliance requirement with these guidelines would not change or be significantly impacted by the anticipated Brexit process.
To further international compliance with the standards, the FATF conducts peer reviews for its members to assess the level of their implementation of the FATF recommendations. These mutual evaluations aim to analyse each country’s ability to prevent criminal abuse of their financial system.

The October 2016 FATF Report to the G20 Finance Ministers and Central Bank Governors outlines the current global agenda on AML/CFT which is intended to inform the regional agendas. The overall objective is to reinforce the FATF’s work on counter-terrorist financing measures in five (5) key policy objectives: 1) Identifying best practices and opportunities to improve effective use of financial intelligence; 2) Ensuring that the FATF standards provide effective tools against terrorist financing; 3) Assisting countries in effectively applying the tools; 4) Monitoring and advocating for urgent progress on remedial action, especially in the fifteen (15) jurisdictions which have strategic deficiencies; 5) Promoting effective cooperation and coordination.

The Caribbean Financial Action Task Force (CFATF) is one of the nine (9) FATF Style Regional Bodies (FSRBs) that exist across the world. Although autonomous from each other, the FATF and the FSRBs share the common goal in combating money laundering and terrorist financing and in fostering effective AML/CFT systems. FATF and FSRBs operate on the basis of (mutual or joint or common) recognition of their work, which implies that FSRBs and FATF put in place similar mechanisms for meaningful participation and involvement into each other’s activities.

The CFATF was created by virtue of the Kingston Declaration in November 1992 and began operations at the Secretariat in 1994. Its establishment was encouraged by the Financial Action Task Force (FATF) with the objective to spread the commitment to confront and defeat money laundering as a consequence of drug trafficking and transnational organised crime to all corners of the globe.

The CFATF has twenty-five (25) members (not including the Dominican Republic as it is a member of GAFILAT - El Grupo de Acción Financiera de Latinoamérica). CFATF is the only organisation in the Caribbean Basin Region that has the mandate to undertake the specialist responsibilities of monitoring regional compliance with the FATF Standards. In this regard the CFATF has undertaken three (3) Rounds of Mutual Evaluations and in January 2015 embarked upon the Fourth Round of Mutual Evaluations which is due to continue to 2022. These assessments have begun globally and are generally seen as more onerous than the previous rounds as they are very resource intensive in human and financial terms.

Component C – Asset Recovery and Cybercrime

A number of CARIFORUM Member States have enacted asset recovery legislation and have included in some instances civil asset recovery. Scarce resources and limited capacity to set up necessary structures and programmes have rendered these national efforts largely ineffective. There is a need to build capacity of law enforcement professionals who can be tasked with the responsibility of investigating, tracing, seizing, forfeiting and confiscating criminal assets. Information sharing, pooling resources and building capacity should further be supported at regional level to promote national recovery of assets efforts.

International networks have been set up for experts in the field of asset tracing, freezing and confiscation. The members of the Camden Assets Recovery Interagency Network (CARIN) include all twenty-eight (28) EU Member States as well as nine (9) international organisations. Similar networks have been created for West Africa, Eastern Africa, Southern Africa, Asia and the Pacific, and Latin America.

CARICOM in conjunction with the United Nations Office on Drugs and Crime (UNODC) and under the auspices of the Regional Anti-corruption Academy for Central America and the
Caribbean, drafted the Agreement for the Sharing or Return of Recovered Assets. The Agreement supports the Caribbean Mutual Legal Assistance Treaty which aims at providing the legal framework for the sharing or return of recovered assets among CARICOM members. This Agreement is intended to aid Member States to use Proceeds of Crime legislation which will strip criminals of their illicit wealth and remove their access to the financial system as well as expose the criminal activities hidden behind legitimate fronts. It is in its final stages of approval and adoption among Member States.

Additionally, an Asset Recovery Informal Network (ARIN) - CARIBE has been set up recently in the Caribbean region as a joint effort between the United States Bureau of International Narcotic and Law Enforcement Affairs (INL), Regional Security System Asset Recovery Unit (RSS ARU), IMPACS, and CFATF (financed by OAS in the first year) in order to provide a platform for informal sharing among investigators and judicial officers on cross border financial and other crimes which will allow for asset recovery.

**Cybercrime** has evolved into one of the fastest growing forms of crime and a significant global challenge for the rule of law across criminal jurisdictions. It has emerged as a particular criminal activity that threatens citizens, businesses, governments and critical infrastructures alike in parallel to the increased digitalisation and broad use of information communication technology.

Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrimes can be categorised as:

- Traditional offences committed online (e.g. fraud, forgery, and identity theft)
- Offenses unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)
- Content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences

In addition to the above categories, **electronic evidence** can be an issue for any crime where emails, and other data stored on computer devices are relevant for investigation and prosecution purposes.

The more real-world crime involves e-evidence, the greater the chances that any law enforcement officer, prosecutor or judge will come across and need to have the skills to deal with e-evidence.

**The fight against cybercrime is a basic tenet of any comprehensive effort and strategy to increase cybersecurity** which is a broader framework commonly referring to the safeguards and actions that can be used to protect the cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. As cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein, there are clear spill-over issues between the two fields that are often overlapping and mutually reinforcing. Cybersecurity strategies aim to build the security, resilience and reliability of Information Communication Technologies (ICT). Cybercrime strategies are more focused on an effective criminal justice response to crimes targeting or using ICT.

Societies are increasingly reliant on ICT which makes them vulnerable to cybercrime. Cybercrime presents a threat to individuals as well as to states and societies as a whole. Building capacity to address cybercrime is a vital part of an overall cybersecurity strategy. A comprehensive legal substantive and procedural legal framework that is based on common standards and allows for effective international cooperation is considered as the minimum foundation in tackling cybercrime. The **Council of Europe’s Convention on Cybercrime** (also referred to as “the Budapest Convention”) which entered into force in 2004 is the only international binding instrument on cybercrime and also serves as a blueprint for any country that wishes to develop its national
legislation in this field. The Convention includes safeguards that aim to protect and uphold human rights while promoting stronger rule of law enforcement and international cooperation on cybercrime. The principles outlined in the convention correspond to EU core human rights values, such as the protection of fundamental rights, freedom of expression, personal data and privacy. Ensuring that adequate human rights safeguards are incorporated is central to all EU engagement on cybercrime and cybersecurity issues. To date, the Dominican Republic is the only country in CARIFORUM that has signed and ratified the Convention while there are countries in the region that have elaborated with the Budapest Convention as their blueprint (indicatively: Jamaica, Dominica).

Another key challenge faced by countries everywhere is that the evolution of cybercrime techniques has accelerated rapidly and the criminal justice actors, mainly law enforcement, judges and prosecutors, have limited capacities to apply cybercrime and electronic evidence legislation in practice to effectively investigate, prosecute and adjudicate such cases. Specific skills are needed within the criminal justice chain, coupled with awareness raising for decision makers and as well as for IT professionals working in both the public and private sector. As cybercrime is a transnational threat it is imperative to promote regional and international cooperation which necessitates a level of harmonisation of national legislation with international standards. It further requires a multi-stakeholder approach including decision makers and parliamentarians, government agencies, private sector representatives, academic institutions, international and regional institutions.

Cybercrime is deemed as an immediate and significant threat in the CARICOM Crime and Security strategy and in the CARICOM Strategic Plan for the Caribbean Community 2015-2019. Cybercrime is also included in the Joint Caribbean-EU Strategy as an area of specific concern to both regions.

Examples of reported occurrences of cybercrimes committed in the CARICOM region include:

- Cyber-attacks to governments’ intranet systems, posing threats to the portals for sending and receiving emails also resulting in system crashes and login problems;
- Hacking of governments’ official websites, attacks on ministry websites, tertiary institutions and private institutions wherein items of data from the website, including usernames, emails and encrypted passwords, were leaked and dumped online;
- Automated Teller Machine (ATM) skimming scams conducted by thieves using well-hidden cameras to capture the personal identification numbers of some customers’ debit and credit cards, from a few major banking institutions;
- Attempted domain hijacking and fake antivirus
- Reported net annual losses of millions of dollars due to cybercrimes, outstripping the front running narcotics crimes in some cases.

In some cases, national actions have been taken to enact legislation to provide criminal sanctions for the misuse of computer systems or data and to facilitate the investigation and prosecution of cybercrimes. However, even where cybercrime legislation has been enacted, the prosecution level remains low due to lack of capacity and knowledge on how respond to cyber and cyber-enabled crime.

### 1.1.1 Public Policy Assessment and EU Policy Framework

The European Commission adopted its Fourth Anti-Money Laundering Package in May 2015. In December 2015, the Commission proposed a Directive on combatting terrorism which criminalises terrorist financing and the funding of recruitment, training and travel for terrorism purposes. At the beginning of 2016 the Commission approved an Action Plan calling for increased efforts in a number of areas to combat terrorism financing. The Commission specifically endorses the work
under way, in particular by the United Nations and the Financial Action Task Force (FATF). The European Commission also committed to actively contribute to the work of the Financial Action Task Force (FATF) as well as to the implementation of its recommendations.

The proposed action is strongly aligned with the Caribbean Regional Indicative Programme (CRIP) Logical Framework and specifically with Result 3.1 "Levels of compliance with FATF AML/CFT Global Commitments to Tax Information Exchange and Transparency increased". As possible operations under this Result, the CRIP explicitly mentions that the EC will assist the region in 1) Supporting Mutual Evaluations, National Risk Assessments and Anti-Money Laundering measures, combatting the financing of terrorism and improving tax information exchange and transparency; 2) Strengthening the capacity of Financial Investigators, Analysts and Supervisors at Financial Intelligence Units; 3) Supporting outreach and public education programmes; and 4) Support the implementation of the Work Plan that has been developed as result of the National Risk Assessments as well as the Improvement Plan AML/FT System following the Fourth Round of Mutual Evaluation. As objectively verifiable indicators, the CRIP mentions the level of compliance with the FATF Recommendations during the Fourth Round of Mutual Evaluations (with the specific target of moving from an average compliance rate of 40% to at least 75% - although this might have to be adjusted in view of the new methodology of the Fourth Round), the number of common exercises and number of persons trained and the number of national and regional institutions supported in public education and awareness raising/advocacy activities on AML/CFT and corruption.

The action is also fully consistent with the EU-CARIFORUM Partnership Strategy adopted in November 2012. The strategy specifies that areas of specific concern to the Caribbean and the EU should include "the promotion of cooperation and collaboration between the Caribbean Financial Action Task Force (CFATF) and partner institutions, and the promotion of and compliance with Internationally agreed standards of transparency and tax cooperation".

The proposal is in line with important policy objectives of the EU as well as the Caribbean spelt out in a number of different documents including the EU Strategy on Citizen Security in Central America and the Caribbean, the aforementioned European Commission Action Plan for strengthening the fight against terrorist financing launched in February 2016, the European Agenda on Security as well as the CARICOM Crime & Security Strategy (CCSS) adopted in 2012.

Cybercrime is an issue of growing concern in the CARIFORUM region. In the CARICOM Crime and Security Strategy, adopted in 2013 by the conference of Heads of Government of CARICOM, cybercrime is listed under the “Tier 1 – Immediate Significant Threats” with strategic goal 8 being “Strengthening CARICOM’s Resilience to Cyber Crime”. CARICOM is seen as becoming increasingly susceptible to cyber-attacks and while presently most cybercrimes originate from countries outside the region, there is a clear risk that the Caribbean region could emerge as a potential base for cybercriminals due to the region’s lack of resources and trained personnel, as well as due to gaps in regulatory systems and enforcement mechanisms. In 2012, a Caribbean Cyber Security Framework was developed by the Organisation of American States (OAS) and the Caribbean Telecommunications Union (CTU). It encompasses four strategic areas: 1. Awareness and Capacity Building, 2. Technical Standards and Infrastructure, 3. Legal Environment and 4. Incident Response and International and Regional Cooperation.

Further to the framework, the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) was developed as a coordinated effort between CARICOM IMPACS, the Caribbean Telecommunications Union (CTU), the Organisation of American States (OAS) and the Commonwealth Secretariat. This action plan seeks to address the cybersecurity vulnerabilities in
each participating Caribbean country and to establish practical, harmonised standard of practices, systems and expertise for cybersecurity, to which each Caribbean country could aspire. It also seeks to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of cybercrime and possible linkages to other forms of criminal activity. This action plan which builds upon the Caribbean Cyber Security Framework identifies five (5) priority areas of intervention for addressing cybersecurity and cybercrime issues in the CARICOM region.

1. Public awareness;
2. Building sustainable capacity;
3. Technical standards and Infrastructure;
4. Legal Environment; and
5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building.

The CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) was approved by the CARICOM Council of Ministers responsible for National Security and Law Enforcement (CONSLE) in November 2016 and by the CARICOM Heads of Government in February 2017.

In the Strategic Plan for the Caribbean Community 2015-2019 cybercrime is listed as an obstacle and threat to social and economic development in CARICOM. Strengthening cybersecurity is seen as a strategy to achieve technological resilience but is also linked to strategies needed to achieve social resilience and citizen security. Steps outlined include capacity building for professionals in the law enforcement and judiciary and the establishment of a CARICOM Cyber Crime Centre and a CARICOM Emergency Response Team.

The objectives of the project are also fully consistent with the strategic objectives outlined in the Caribbean Regional Indicative Programme (CRIP) for the 11th European Development Fund (EDF). In particular, the proposed project supports the implementation of Focal Area 3: Crime and Security, in line with the three specific objectives: 1) Crime Prevention, Risk Reduction and enhancement of Restorative Justice, 2) to Enhance Citizen and Border Security and 3) Increasing compliance with international norms on financial crimes, terrorism financing and corruption. Strengthening regional capacity to fight cybercrime also builds cybersecurity in the region which is in support of CRIP Focal Area 1: Regional Economic Cooperation and Integration as strengthened ICT systems promote a stronger business and investment climate.

In the Joint Caribbean-EU Strategy, adopted in 2012, cybercrime (including identity theft and copyright infringement) is included as an area of specific concern to both regions. The strategy further specifies that the Caribbean-EU common fight against crime must include cooperation with the UN, Interpol, Europol, OAS, IMPACS and other regional organisations.

The Cybersecurity Strategy of the European Union, adopted in 2013, goes beyond promoting cybersecurity within the EU to include the development of capacity building measures and resilient information infrastructures in third countries. It specifies that EU aid instruments should be used for cybersecurity capacity building measures such as promoting the Budapest Convention to address cybercrime, training of law enforcement, judicial and technical personnel as well as to give support to national policies, strategies and institutions in third countries. The objective for the EU to support third countries in the fight against cybercrime is further reiterated in the EU Strategy on Citizen Security in Central America and the Caribbean. Additionally, the project is in line with the EU-CELAC Action Plan under the umbrella of citizen security by promoting and strengthening action related to awareness raising, mutual confidence and understanding concerning the issue of citizen security. It will also seek to strengthen cooperation between the EU and the region in relation to capacity building, transfer of technology and methodologies in the area of crime detection.
The proposed project is conformant to EU aid effectiveness commitments under the Paris Declaration on Aid Effectiveness (2005) and the Accra Agenda for Action (2008).

1.1.2 Stakeholder analysis

The implementation of the project will necessitate engagement with a wide array of stakeholders from public and private sectors. Key stakeholders for all project components will be the competent government authorities.

Component A – Implementation of the Mutual Evaluation Programme

Component B – National Risk Assessments and National Action Plans

Key stakeholders for Components A and B will be the competent government authorities in the CARIFORUM Member States, including Ministries of Finance, Justice, Interior and Foreign Affairs of the Member States.

Further stakeholders include:

- Financial Intelligence Units
- Customs service, border agencies, and where relevant, trade promotion and investment agencies.
- Task forces or commissions on money laundering, financing for terrorism or organised crime.
- Supervisors of financial institutions, including the supervisors for banking and other credit institutions, insurance, and securities and investment.
- Supervisors or authorities responsible for monitoring and ensuring AML/CFT compliance by other types of financial institutions, in particular bureaux de change and money remittance businesses.
- Exchange agencies for securities, futures and other traded instruments.
- Central Banks/other regulatory bodies.
- The relevant financial sector associations and financial institutions (including both senior executives and compliance officers, and where appropriate internal auditors).
- External auditors.

The private sector will also be engaged in the design and implementation of the actions. These will include Designated Non-Financial Businesses and Professions (DNFBP) – i.e. non-financial businesses and professions in casinos, real estate agencies, precious metals/stones businesses as well as lawyers, notaries and accountants. Furthermore media and civil society are valuable stakeholders for awareness raising activities as the components will include visibility/communications strategies in order to strengthen awareness on AML/CFT issues.

Component C – Asset Recovery and Cybercrime

The key stakeholders in the region for the capacity building on Asset Recovery are the Financial Intelligence Units and the newly formed Asset Recovery Informal Network ARIN-CARIBE. In identifying support activities for the ARIN-CARIBE, close coordination will be sought with the United States Bureau of International Narcotic and Law Enforcement Affairs (INL), RSS Asset Recovery Unit (RSS ARU) and OAS.

On cybercrime capacity building, key stakeholders will be the law enforcement and judiciary professionals from the CARIFORUM Member States. Legislators will also benefit from trainings on cybercrime to facilitate legislative review and possible reform. To ensure sustainability, training institutions will be important stakeholders as the programme will support the design and development of cybercrime training modules to be incorporated in educational institutions in the region. While a thorough mapping and educational design strategy will be part of the project
activities, beneficiaries already identified include the University of the West Indies, the Regional Police Training Centre (in Barbados) and national police training schools (through a regional approach).

Regional stakeholders include the Caribbean Community Implementation Agency for Crime and Security (CARICOM/IMPACS) as the coordinator of the regional Action Plan on Cybercrime and Cybersecurity which will receive technical assistance to promote its effective coordination of initiatives on cybercrime/cybersecurity in the region. The Regional Intelligence Fusion Centre (RIFC), a sub-section of CARICOM/IMPACS will receive training and capacity building as it relates to cybercrime in the area of strategic analysis to allow for a regional approach and to allow for the creation of linkages to other possible criminal activities, thus significantly improving its intelligence product (particularly in areas such as transnational crime), for action within the CARIFORUM Member States. Additionally, National Intelligence Points of Contacts in Member States will be targeted alongside RIFC staff to receive training with respect to the gathering and monitoring of cybercrime information and intelligence. This will also support the work of the Regional Cyber Committee and the Establishment of a Regional Capacity Centre for Cyber Security and Incident Response as outlined in the CCSCAP.

Decision makers, parliamentarians and other professionals employed in selected government ministries who will benefit from awareness raising efforts and training on asset recovery and cybercrime. The private sector will be involved, especially the Internet Service Providers in relation to their cooperation with law enforcement in the fight against cybercrime, and the private owned critical infrastructure for any overlaps pertaining to cybersecurity. The projects will include visibility/communications strategies in order to strengthen awareness on AML/CFT issues and cybersecurity/cybercrime. This cybercrime communications strategy will also aim to promote reporting on cybercrime, including child online abuse and cyber violence against women and girls (cyber VAWG). Media and civil society are valuable stakeholders for these awareness raising activities.

An important stakeholder for coordination purposes will be the stakeholders’ network, involving CARICOM IMPACS, Commonwealth Secretariat, the Caribbean Telecommunications Union (CTU) and the Organization of American States (OAS).

The project component will further seek to engage those CARIFORUM Member States who have advanced legislation and/or capacity on cybercrime as "regional champions" to promote inter-region cooperation and share context-relevant lessons learnt. The Dominican Republic can play an important role as it is a ratifying state of the Budapest Convention and also has an advanced regulatory framework on cybercrime. Similarly Jamaica could contribute its experiences with its legislation that is in line with the Budapest Convention and considerable expertise/capacity on cybercrime forensics.

1.1.3 Priority areas for support/problem analysis

Component A – Implementation of the Mutual Evaluation Programme

The average compliance rate under the Third Round of Mutual Evaluations in the Caribbean Region was only 40%. This situation leaves the CARIFORUM Member States with the challenges of tackling the needs and gaps at regional and national levels to boost the levels of compliance while adapting to and effectively engaging in the new methodology of the Fourth Round of Mutual Evaluations. This new methodology will not only assess whether the necessary laws, regulations or other required measures are in force and effect and whether the supporting institutional framework
is in place, but also, with its new effectiveness component, examine whether the AML/CFT systems are working, and the extent to which the countries are achieving the defined set of outcomes.

This component therefore seeks to provide support to CARIFORUM Member States to prepare, carry out and follow-up on the ongoing Fourth Round of Mutual Evaluation Missions which are supposed to produce high quality reports that will withstand the rigorous regional and international scrutiny of the global Quality and Consistency review process.

As part of its core mandate, CFATF will implement the Mutual Evaluation Programme. Key costs associated with the Mutual Evaluation Missions that will need to be covered by the Programme, will be mainly travel, accommodation and per diem costs of the experts/assessors. Half of the costs of the missions will be borne by the Member States that are to be evaluated, and half by the Programme. The CFATF Project Team will assist with the provision of a training package. This will include Standards Training, Assessors Training, Pre-Assessment Training Seminars, Typology Exercises, Legislative Drafting as well as specialist guidance on Terrorist Financing and Proliferation. Emphasis will be placed on selection of beneficiaries for these trainings to ensure that they hold positions where the skills can be used as intended by the programme and to ensure sustainability of the programme activities.

Component B – National Risk Assessments and National Action Plans

To further strengthen the level of financial compliance in the Caribbean region, support will be provided to implement National Risk Assessments in consultations with key stakeholders, andpartnership with CFATF. National data capturing mechanisms which are essential to justify the risk based approach to implementing the FATF Recommendations will also be upgraded.

This component will also include the design of National Action Plans which would address all outstanding deficiencies found in past Mutual Evaluations and Follow-up Reports, and refer to those legal, regulatory and institutional measures that must be put in place so that the national AML/CFT infrastructure is in keeping with all FATF Recommendations. The National Action Plans will seek to ensure that the necessary reforms in keeping with the requirements of the Fourth Round of Assessments in preparation for the Mutual Evaluation Missions and rectification of identified deficiencies thereafter are expeditiously implemented. Preparation of the National Action Plans will also require the involvement of a wide and diversified range of national stakeholders and will be assisted by specialised agencies in the EU with previous experience of international cooperation in this sector. National Action Plans will need the investment of significant political capital to materialise, especially when a change of the legislative and regulatory framework will have to be adopted. Outreach campaigns targeted at political decision makers, the private sector, civil society and the general public will need to be launched.

Support will be given to the establishment of a strong continuous monitoring system which will oversee not only the implementation of the plans, but more generally financial compliance standards throughout the region. The CFATF Vision 2022 platform will maintain an easily accessible central database of the FATF Recommendations and Interpretative Notes, the AML/CFT Methodology, legislation, regulations, guidance notes and all documentation relevant to the assessment process, including the comments and amendments by each Assessor on each Mutual Evaluation Report. This will expedite the consultative mechanism between those CFATF Members being assessed, the Assessment Teams and the CFATF Secretariat and allow the Mutual Evaluation
Assessors, Assessed Country and Reviewers to work simultaneously in one document so as to draft, finalise and present high quality Mutual Evaluation Reports.

Additionally, assistance will be given for the implementation of Work Plans that have been developed as result of National Risk Assessments as well as the Improvement Plans AML/FT System emanating from the Fourth Round of Mutual Evaluations.

**Component C – Asset Recovery and Cybercrime**

Asset recovery actions form an important part of the global effort to address AML/CFT issues. The FATF Recommendations require jurisdictions to implement measures that will freeze, or if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant United National resolutions. As noted earlier, a number of CARIFORUM Member States have enacted asset recovery legislation and have included in some instances civil asset recovery. Scarce resources and limited capacity to set up necessary structures and programmes have rendered these national efforts largely ineffective. The programme will therefore seek to build capacity of law enforcement professionals who can be tasked with the responsibility of investigating, tracing, seizing, forfeiting and confiscating criminal assets. Information sharing, pooling resources and building capacity should further be supported at regional level to promote national recovery of assets efforts. It is therefore also envisaged that the programme will engage closely with as well as support the newly established ARIN-CARIBE network of investigators from law enforcement in the region.

The existing capacity of the CARIFORUM Member States to address cybercrime varies from country to country. Some countries are further along in their legislative efforts to counter cybercrime, such as the Dominican Republic who already has enacted a regulatory framework on cybercrime and moreover has ratified the Budapest Convention. The Dominican Republic is a member of CARIFORUM, but not of CARICOM or CTU. Early discussions on the project with the Dominican Republic showed that they would consider their participation both as beneficiary and as a resource to the project as they have already enacted a regulatory framework on cybercrime and moreover have ratified the Budapest Convention. Potential synergies with the GLACY+ project would need to be explored as the Dominican Republic may function as a regional hub for the continuation of GLACY activities in the region (see more on GLACY in point 3.2 on complementarity, synergy and donor coordination). Other countries, such as Jamaica and Trinidad and Tobago, have established dedicated law enforcement units with more targeted experience and knowledge on cybercrime. While a regional approach is necessary to maximise resources and ensure regional collaboration on cybercrime, the envisaged support would have to address the countries’ individual needs.

The outcome of the most recent regional stakeholders meeting held in Saint Lucia in March 2016 included a joint communication that highlighted the need for criminal justice and information communication technology expertise. This need was also identified in the five (5) needs assessments done by the Commonwealth Secretariat, under its Commonwealth Cybercrime Initiative (CCI). These assessments were done on the existing capacity to combat cybercrime in five (5) Commonwealth member states; Antigua and Barbuda, Barbados, Dominica, Grenada and Trinidad & Tobago. As agreed in the Saint Lucia discussions, the Caribbean region needs skills to be developed on prevention, detection and prosecution of cybercrime as well as skills to build the security of national networks. Crucially, the approach would have to be sustainable and continuous.

---

2 Gros Islet Communique, the Caribbean Stakeholders Meeting on Cybersecurity and Cybercrime (CSM-II), Saint Lucia 16-18 March 2016.
as cybercrime/cybersecurity expertise is constantly in need of “upgrading” in view of its changeable nature. This is also substantiated by the Cyber Security and Cybercrime Action Plan CCSCAP.

This component has four (4) main scopes of engagement – legislation review and update to meet international standards; capacity building/training of law enforcement, judiciary and legislators including through incorporation of cybercrime/cybersecurity modules in selected national and regional educational institutions; engagement and awareness raising of decision makers, parliamentarians, public sector ICT professionals and private sector representatives; and strengthened regional capacity to coordinate efforts to counter cybercrime through support to the RIFC and IMPACS in implementing the CCSAP.

Throughout the project activities, particular focus will be given to ensuring human rights safeguards in compliance with international standards and best practices. The project will make use, where applicable, of existing international guidelines developed for capacity building on cybercrime and cybercrime legislation.

Special emphasis will be placed on ensuring sustainability of the trainings developed for law enforcement and judiciary. Training modules developed and designed specifically for inclusion into existing educational programmes for law enforcement and judiciary will be a concrete output of the project. Early liaison with relevant regional educational institutions will be imperative to ensure ownership and support for these modules.

Insufficient reporting and lack of awareness have been identified by CARICOM as challenges contributing to cybercrime in the region. The project’s support to regional coordination and exchange on cybercrime would promote a greater situational awareness. The technical assistance to CARICOM/IMPACS will strengthen the agency’s ability to raise awareness on cybercrime with the region’s Ministers of National Security and with CARICOM and CARIFORUM secretariats. The project’s visibility strategy will further aim to raise awareness with citizens in the region, including on issues pertaining to child online abuse and on measures to promote child online protection.

A particular aspect of the cybercrime dimension is in relation to gender. Cyber-violence against women and girls is emerging as a global problem with serious implications for societies and economies around the world. Cyber violence against women and girls (cyber-VAWG) is under-reported both in western countries with high internet penetration as well as in the Global South. This emerging trend requires a gender sensitive development of the response to cybercrime, not only at the stage of legislation but also in the investigation, prosecution and adjudication of crimes entailing cyber-VAWG. To this end, the Cybercrime Convention Committee established a new working group on "cyberbullying and other forms of online violence especially against women and children" in November 2016. The first report and recommendations are expected in late 2017, which could be taken up by the proposed action.

2. Risks and Assumptions

<table>
<thead>
<tr>
<th>Risks</th>
<th>Risk level (H/M/L)</th>
<th>Mitigating measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of Member States to bear costs of</td>
<td>M</td>
<td>Political dialogue through CARICOM and at national level</td>
</tr>
<tr>
<td>CFATF Missions as M</td>
<td></td>
<td>on importance of AML/CFT</td>
</tr>
</tbody>
</table>

3 There are six broad categories that encompass forms of cyber-VAWG and fall under different elements of cybercrime or cyber-enabled crimes: hacking, impersonation, surveillance/tracking ("cyber-stalking"), cyber-harassment, use of the internet to lure potential victims into violent situations (ex. trafficking); and malicious distribution (ex. "revenge porn").
expected

Varying levels of AML/CFT and cybercrime capacities in Member States which may lead to difficulties in designing and delivering regional training modules

Strengthened measures on AML/CFT negatively impacts financial inclusion in the Caribbean.

Strengthened law enforcement on cybercrime encroaches on human rights (such as right to privacy).

Duplication and overlapping of training initiatives

Weak institutional capacity to absorb the assistance provided and to trickle down to national level

Lack of gender awareness, gender sensitivity, gender understanding increase existing gender inequality.

This risk can be mitigated through a flexible context-driven approach to the trainings.

FATF guidance will be applied on AML/CFT and Financial Inclusion + a social dialogue with be held through engagement with media and civil society stakeholders to exchange on the impact of measures taken on citizens in the region.

Internationally accepted principles will be advocated from the start with strong emphasis that fundamental human rights values must be at the core of all project activities with risk mitigation strategy developed.

Coordination and exchange with all stakeholders in the region

Tailored approach based on good initial assessments and flexibility in implementation

Include gender analysis and gender desegregated data. Make sure there is gender balance among beneficiaries of the action.

**Assumptions**

Continued commitment of CFATF countries to the Mutual Evaluation Missions.

Timely engagement of European and international specialised agencies (such as EUROPOL, EUROJUST, CARIN network)

Sufficient political engagement by CARIFORUM/CARICOM Member States to enable required changes of the legislative and regulatory frameworks.

Sufficient willingness by universities and other educational institutions (for law enforcement and judiciary) to adopt modules on cybercrime/cybersecurity as this is vital in order to ensure the sustainability of the capacity building trainings.

Ability of participants in project training activities to translate acquired knowledge into actions, thereby strengthening the capacity of the criminal justice chain.
3. LESSONS LEARNT, COMPLEMENTARITY AND CROSS-CUTTING ISSUES

3.1 Lessons learnt

EU funding has already been used to support law enforcement agencies in the Caribbean, with main emphasis on drug control. Additionally, the Caribbean region has been able to benefit from EU funding to global programmes lending support to capacity building to counter organised crime and drug trafficking.

The 1998-2002 EU "Caribbean Regional Anti-Money Laundering Programme" financed together with the US and UK, provided EUR 4 million for building institutional capacity to reduce money laundering in the Caribbean region. CFATF was the main beneficiary of these capacity building efforts. While the evaluation of the programme was largely positive (see ROM report in 2002) it was recommended to ensure regionally sourced funding for CFATF activities to avoid full dependency on outside donors.

In its enlargement process, the EU has gathered considerable experience with support to Financial Intelligence Units (FIUs) and capacity building on the enforcement side through twinning arrangements and would be happy to contribute this expertise to an intervention. Lessons learnt may also be drawn from similar interventions on financial compliance such as the new EU funded AML/CFT Global initiative (EUR 16 million; AAP 2016) which is targeting the South East Asia (SEA) region, notably Indonesia and the Philippines (and Lao PDR, Myanmar, Vietnam, Thailand, and Cambodia) as well as the Middle East and North Africa (MENA) region (with the following target countries: Jordan, Lebanon, Tunisia, Iraq, Egypt, Algeria, Morocco, Libya and, as appropriate, Iran). The EU has supported a number of regional initiatives, including the Financial Action Task Force of South America (GAFILAT) which includes the Dominican Republic as a member.

The GAFILAT-EU project spanned 90 months, from December 2009 – June 2017. Main activities included the assessment of current situations and legislations in place to prevent money laundering in the non-banking financial sector in GAFILAT Member States; strengthening of administrative, judicial and law enforcement cooperation to fight money laundering; assessment of the current capacity to meet the investigation needs; promoting inter-institutional coordination and multidisciplinary working groups; improvement and standardization of the existing investigation capacities; strengthening of police and judicial cooperation to fight asset laundering; establishment of cooperation agreements and opportunities with other countries and/or regional groups; and the promotion of implementation at national level of the new international standards and train the experts in charge of future mutual evaluations. Lessons learnt from the GAFILAT-EU project will be taken into account for the implementation of the programme in reference. As an example, the 2012 Mid Term Review found that there was little progress in trans-regional collaboration, i.e. that GAFILAT did not engage in a significant manner with its neighbouring regional organisations CFATF and Inter-Governmental Action Group against Money Laundering in West Africa.

---

4 Predating the 9th EDF (1975-2001) support in the total amount of EUR 25 million was given to the Regional Drug Law Enforcement Training Centre (REDTRAC) in Jamaica, the Regional Police Training Centre (RPTC) in Barbados, the Inter-Agency Drug Control Training Centre (CIFAD) in Martinique and the Regional Search Centre (RSC) in Jamaica. Under the 9th EDF 2002-2007 the Caribbean Integration Support Programme (CISP) allocated EUR 2 million for the continuation of the 1996-2001 Barbados Plan of Action (Regional Plan of Actions on Drugs) and EUR 1 million in support of the newly developed IMPACS. Under the 10th EDF CRIP 2007-2013, a total amount of EUR 12.2 million was allocated to drug supply control and crime prevention. Main implementing parties included IMPACS, RSS, CFATF and CARIFORUM.

5 Such as GIABA, the Inter-Governmental Action Group against Money Laundering in East Africa; a CFT Programme in the Horn of Africa implemented by CIVI.POL Conseil; the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG); and le Groupe d’Action contre le blanchiment d’Argent en Afrique Centrale (GABAC) in West Africa.
(GIABA). However, it was deemed successful in achieving the regional goals of strengthened financial compliance in GAFILAT Member States. There is an opportunity for this programme to include CFATF-GAFILAT joint activities, also through the programme activities benefitting the Dominican Republic, a member of GAFILAT (developed further under 3.2).

While a number of CARIFORUM Member States in response to increased phenomena of financial crimes have enacted asset recovery legislation and have included in some instances civil asset recovery, scarce resources have severely hampered the establishment of necessary structures and programmes. There is a prevalence of unskilled and untrained persons in law enforcement that are tasked with the responsibility of investigating, tracing, seizing, forfeiting and confiscating criminal assets. Many acts of seizures do not run the full extent of prosecution as untrained investigators sometimes breach the perpetrators’ rights or use improper methods which give way to failed cases or return of assets. Judicial officers do not have much experience in this subject area. The network of regional investigators will seek to address this.

Previous support to cybersecurity in the Caribbean has to a large extent focused on the development of model laws on cybercrime, including the Commonwealth Model Law, the International Telecommunications Union (ITU) (EDF funded) Model Laws for the ACP countries and the World Bank funded OECS Model Law (under the Electronic Government for Regional Integration Project – therefore often referred to as the EGRIP Model Law). Only the Commonwealth Model Law is the result of an official inter-governmental approvals process. As a result of these initiatives, cybercrime/cybersecurity legislation has been enacted in many countries in the Caribbean with variant results in relation to compliance with the international legislative standards set by the Budapest Convention on Cybercrime. According to a 2014 Council of Europe study, the Harmonization of ICT policies and legislation across the Caribbean (HIPCAR) Model Law has influenced legislation in St Kitts and Nevis, Jamaica, Bermuda, Barbados and Trinidad & Tobago. Likewise the Electronic Government for Regional Integration Project (EGRIP Model Law financed by the World Bank) has been largely adopted by Grenada and Dominica, and the Commonwealth Model Law has influenced legislation in Antigua. The CCSCAP will further address a regional approach to the legal environment for cybercrime and cybersecurity.

Lessons learnt have shown that despite enacted cybercrime legislation, there is still need for improvement in prosecution levels, and for further work to build capacity and knowledge on how respond to cyber and cyber-enabled crime. The programme will therefore pursue the update of legislation and train legislators where necessary to meet international standards that also facilitate regional and international cooperation, and develop trainings targeted at the appropriate stakeholders to raise capacity to enforce existing legislation. To achieve more sustainability the trainings will be designed and developed also for inclusion into the curricula of selected regional and national educational institutions.

3.2 Complementarity, synergy and donor coordination

In 2016 CFATF was awarded a direct grant of EUR 1.233 million under the 10th EDF CARIFORUM Crime and Security Cooperation Programme. The objective of the grant was to provide training for financial analysts and investigators from Financial Intelligence Units (FIUs) across the region in investigation techniques relating to transnational criminal activity and financial crime. The implementation of this Grant started in September 2016 and three workshops for financial analysts have been held in 2017. No reports or evaluations are available on the progress to date. The Asset Recovery activities proposed under this action will complement the trainings designed under the previously awarded grant and emphasis will be given to explore synergies between the two programmes. Additionally, CFATF has from its inception in 1992 received

---

6 “Cybercrime Model Laws”, Discussion paper, 23 December 2014, Council of Europe, [www.coe.int/cybercrime](http://www.coe.int/cybercrime)
funding from a range of donor partners in sums ranging from US$25,000 to US$300,000. These donor partners include the Commonwealth Secretariat, the European Union, CARIFORUM, Rand Corporation, Swiss Development Corporation, United Nations Office on Drugs and Crime Policy, the Caribbean Development Bank, the Central American Bank for Economic Integration, Trinidad and Tobago, Canada, France, Spain, Mexico, the Netherlands, United States of America and the United Kingdom. At present there is no other donor supporting the Mutual Evaluations carried out by the CFATF. Close dialogue will continue with donors present in the region to ensure there is no duplication of efforts in the programme’s capacity building activities on financial compliance and asset recovery.

As mentioned earlier, the Financial Action Task Force of South America (GAFILAT) has received EU funds 2009-2017 to support its activities. Linkages already exist between CFATF and GAFILAT. The CFATF Executive Director provided technical assistance and shared experiences for the establishment of GAFILAT and both organisations continue to close working relations on a variety of AML/CFT related topics which will be of benefit to the members of both organisations. The Joint Seminar for the Training of Mutual Evaluation Examiners which was held in Panama in August 2017 and Joint Training Seminar on Terrorist Financing in Bolivia in September 2017 are examples of joint CFATF/GAFILAT collaboration. Continued joint activities will be explored under the programme and the programme's support for the Dominican Republic will form a natural link between the two regional organisations.

The EU has supported the Regional Technical Assistance Centre in the Caribbean (CARTAC) since its establishment in 2001. The latest support of EUR 5 million over the period January 2017 – April 2019 will support CARTAC’s 5th phase which focuses on capacity building in twenty (20) Governments and Territories across the Caribbean region in the implementation of the Basel II and III Accords. Synergies will be sought and discussions are ongoing with IMF/CARTAC on AML/CFT issues in the Caribbean region. It is possible that the IMF through CARTAC could make available AML/CFT expertise as part of future programme activities.

In the area of asset recovery, the United Kingdom (UK) Crown Prosecution Office installed a number of Officers in the region which have assisted mainly the Eastern Caribbean States in enhancing their asset recovery legislation to include civil asset recovery. The UK has also established an Asset Recovery Office within the Regional Security System (RSS) to refine the capacity within the Organisation for Eastern Caribbean States (OECS) sub-region only in an effort to collect and prosecute forfeiture of criminal proceeds.

Canada is supporting an OAS project on asset recovery for the Caribbean which is to be launched in the fall of 2017. Canada will contribute 1.6 million CAD (approx. EUR 1 million) for a period of three years to conduct two regional assessment (one on the current state of asset recovery processes and one on the asset management systems), to hold four regional workshops in the Caribbean and in Central America on asset recovery and asset management, and to develop two guidelines for the Caribbean (on asset recovery and on asset management). The Delegation and CARICOM/IMPACS are liaising with the Canadian colleagues and with the OAS to ensure full complementarity of mutual activities and to explore possible joint actions.

CARICOM through CARICOM IMPACS has partnered with the United Nations Office on Drugs and Crime (UNODC) under the auspices of its Regional Anti-corruption Academy for Central America and the Caribbean and drafted the Agreement for the Return and Sharing of Recovered Assets. This Agreement will aid Member States in the use of Proceeds of Crime legislation which will strip criminals of their illicit wealth and remove their access to the financial system as well as expose criminal activities hidden behind legitimate fronts. This Agreement is in its final stages of
approval and adoption by Member States pending the approval by the Legal Affairs Committee of CARICOM which is foreseen to take place in mid-October 2017.

CARICOM has commenced the drafting of Model Civil Asset Recovery Legislation in conjunction with the RSS Asset Recovery Unit further to a mandate of the Conference of Heads of Government at its meeting in July 2017. The Model Legislation is at an advanced stage of completion and has included review challenges and gaps within existing Member States legislation.

As noted earlier in the document, an Asset Recovery Informal Network (ARIN) has been set up in the Caribbean region as a joint effort between the United States Bureau of International Narcotic and Law Enforcement Affairs (INL), RSS Asset Recovery Unit (RSS ARU), IMPACS, and CFATF (financed by OAS in the first year).

In the field of cybercrime, the Caribbean countries have benefited from a range of ongoing and planned activities. Through the ongoing collaboration with critical agencies such as CARICOM IMPACS, Commonwealth Secretariat, the OAS and the CTU, liaison and close coordination will take place with other regional and international actors throughout the project cycle so as to ensure maximisation of synergies and to avoid duplication of efforts.

The Global Action on Cybercrime (GLACY) project is a joint EU/Council of Europe project that aims to support countries to implement the Budapest Convention. This would enable the national criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence. This project is closing in October 2016 and a second phase of the project, GLACY+, was launched in March 2016 and will run to February 2020. It will expand the engagement of GLACY (which supported seven priority countries in Africa and the Asia-Pacific region – Mauritius, Morocco, Senegal, South Africa, Sri Lanka and Tonga) to also include countries in Latin America and the Caribbean. It is foreseen that the Dominican Republic will be a beneficiary under this project.

The EU, led by EEAS, further supports a capacity building programme under the Global Crisis Room Support Programme (GCRSP). This programme includes regional agencies involved in crisis management in the Caribbean (CARICOM IMPACS; including its sub agencies JRCC & RIFC RSS, CDEMA and CARPHA). A training course on cybersecurity in crisis response has been delivered under this programme in June 2016 by the OAS Inter-American Committee against Terrorism (CICTE). The Delegation is liaising closely with the project team to benefit from the GCRSP project’s experiences and knowledge of the region.

Coordination will also be sought with the El Paccto continental programme (Europa-Latinoamerica Programa de Asistencia Contra el Crimen Transnacional Organizado: Por el Estado de Derecho y la Seguridad Ciudadana) and the COPOLAD II programme (Cooperation Programme between Latin American Countries and the European Union on Drugs Policies).

The Commonwealth Secretariat, through the Commonwealth Telecommunications Organisation (CTO) has developed a Commonwealth Cybergovernance Model with an accompanying Commonwealth Approach for Developing National Cybersecurity Strategies. Additionally, the Commonwealth Secretariat has created a programme on cybercrime, the Commonwealth Cybercrime Initiative (CCI). The aim of this initiative is to provide assistance and build capacity for member states to combat cybercrime. As mentioned earlier in the document, initial needs assessments have been done on the existing capacity to combat cybercrime in five Commonwealth member states; Antigua and Barbuda, Barbados, Dominica, Grenada and Trinidad & Tobago. The results form an integral part of the CCSCAP which emanated from the stakeholders meeting in Saint Lucia in March 2016.
OAS Ministers of Justice or Attorneys General of the Americas (OAS/REMJA) and its Working Group on cybercrime is the principal hemispheric forum to strengthen international cooperation in the prevention, investigation and prosecution of cybercrime; facilitate the exchange of information and experiences among its members; and make necessary recommendations to enhance and strengthen cooperation among the OAS member states and with international organizations and mechanisms. OAS/REMJA organises several regional trainings on cybercrime for judges and law enforcement annually. OAS/CICTE is assisting countries in the region with the development of National Cybersecurity Strategies, policies and the establishment of Computer Emergency Response Teams (CERTS). Next step is to build the capacity of individual states to manage these CERTS in a manner that would benefit the national criminal justice systems in combating cybercrime and to further promote information exchange on the regional and international level. The OAS/CICTE receives funding from Canada and the UK for this project (as well as in-kind expertise from donors like Spain and Estonia).

Canada further funds INTERPOL to give training and equipment in cyber forensics to the Americas, including the Caribbean. Canadian funds have also been given to UNODC to strengthen authorities in Central America (including Belize and the Dominican Republic) to investigate and combat internet crimes against children.

The Delegation has also exchanged with the FBI representative at the US Embassy and while they have delivered some training and given investigation support in response to specific requests, the US Embassy (State Department, FBI and USAID) do not have any current programmes on cybercrime/cybersecurity in the Caribbean but the US implements training activities in the field of cybercrime particularly under the framework of REMJA.

It should be noted that the purpose of the CARICOM Cyber Security and Cybercrime Action Plan is to provide a framework within which all initiatives of Cyber Security and Cybercrime in the region will be developed, implemented and controlled in order to ensure they are properly synchronised, duplication is eliminated and the benefit to the region is maximised.

3.3 Cross-cutting issues

The design of the Financial Compliance/Asset Recovery activities will be in line with the guidance provided by the FATF on AML/CFT measures and Financial Inclusion7. As noted in this guidance, the promotion of AML/CFT standards could negatively impact the access to financial institutions/banking services – often with disproportional impact on vulnerable groups. These vulnerable groups include low income and rural populations, often with women as head of households. This FATF guidance, together with context-specific data on vulnerable groups in the Caribbean countries, will promote a gender and rights-based perspective on design of project activities. Close engagement with media and civil society will also be sought throughout the project’s implementation cycle as a means to promote social dialogue on AML/CFT.

The Cybercrime component will be implemented through a rights-based approach (RBA) with special attention to ensure that human rights form a central part of the project’s capacity building activities. Through RBA the design of activities addresses the capacity gaps of both rights-holders and duty-bearers. The rights-holders, mainly the citizens in the CARIFORUM member states, will be assisted in claiming their rights through raised awareness on cybercrime and cybersecurity, including the issue of child online abuse. Strengthened capacity to detect, prevent and combat

---

cybercrime will aid the duty-bearers (CARIFORUM governments, law enforcement and judiciary) to meet their obligations toward the citizens. Close engagement with media and civil society will be sought throughout the project’s implementation cycle as a means to promote social dialogue on cybercrime and cybersecurity. Gender is an integral part of RBA and further receives a strong focus in the cybercrime component. Stronger capacity to counter cybercrime also includes stronger capacity to counter online sexual abuse of women and children as well as the spread of child sexual abuse material. Child online protection will be integrated into the trainings and the training curricula for law enforcement and judiciary. Child online protection will further be given specific focus in awareness raising and visibility activities. Throughout, a gender sensitive analysis shall make the action more sustainable through: (i) ensuring that national authorities are aware of relevant women’s human rights norms and standards and that they are trained to respect and protect these rights while performing their functions; (ii) supporting the legislative reforms that are gender-sensitive; (iii) promoting the balanced representation of women in the security sector; (iv) fostering the increased participation of women in all operational activities related to the actions; and (v) be at the foundation of the design of trainings, visibility and awareness raising activity, with the aim to address gender specific abuse.

4. DESCRIPTION OF THE ACTION

4.1 Objectives/results and options

The overall objective of all project components is to contribute to the improvement of safety and security in the CARIFORUM region.

This Action is relevant for the Agenda 2030. It contributes primarily to the progressive achievement of SDG Goal 16, and particularly targets 16.4 "By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime", 16.6 "Develop effective, accountable and transparent institutions at all levels" and 16a “Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime". This does not imply a commitment by the countries benefiting from this programme.

Component A – Implementation of the Mutual Evaluation Programme

The specific objective of this component is to strengthen financial compliance in the Caribbean region through supporting CARIFORUM Member States in undertaking the FATF Fourth Round of Mutual Evaluation Missions.  

Component B – National Risk Assessments and National Action Plans

The specific objective of this component is to strengthen financial compliance in the Caribbean region through supporting CARIFORUM Member States in carrying out National Risk Assessments as well as to design and implement National Action Plans. Additionally support will be given to Work Plans that have been developed as result of National Risk Assessments.

Components A and B are closely interlinked and mutually reinforcing. The estimated results for these two components are:

---

8 See annexed the CFAT indicative calendar for Mutual Evaluation Missions, and the CFATF compliance table
1. Increased levels of compliance with FATF AML/CFT and Proliferation Financing Recommendations, as well as global commitments to tax information exchange and transparency.
2. Enhanced efficiency and effectiveness in fighting corruption, bribery and white collar crime including money laundering.
3. Improved monitoring and regulation of the informal financial sector and the control of cash flows

Component C – Asset Recovery and Cybercrime

The specific objective is to strengthen the capacity of CARIFORUM Member States on asset recovery and cybercrime, in compliance with international standards and the rule of law. The estimated results are:

1. Enhanced capacity on asset recovery at national level in CARIFORUM Member States.
2. Strengthened national and regional coordination and cooperation on asset recovery activities through the ARIN-CARIBE network.
3. Increased compliance with international standards on cybercrime (as prescribed in the Budapest Convention on Cybercrime).
4. Increased due-process compliant capacities of criminal justice authorities (police, judiciary) to investigate prosecute and adjudicate cases of cybercrime and electronic evidence and engage in effective inter-agency, public-private and international cooperation.
5. Increased awareness and capacities amongst decision makers, parliamentarians, relevant national authorities including public service ITC professionals on cybercrime and cybersecurity policies.
6. Strengthened regional coordination of cybercrime/cybersecurity activities through IMPACS as the main coordinating agency for the implementation of the CCSCAP, including capacity building for IMPACS and the Regional Intelligence Fusion Centre (RIFC).

4.2 Main activities

Component A – Implementation of the Mutual Evaluation Programme

Specific activities are planned to include inter alia, and not limited to:

- Series of trainings for Member State representatives including Standards Training, Assessors Training, Pre-Assessment Training, Typology Exercise Training, Legislative Drafting Training as well as specialist guidance on Terrorist Financing and Proliferation
- Organise national pre-assessment workshops
- Undertake Mutual Evaluation Missions of Member States
- Plenary discussion and adoption of Mutual Evaluation Report (MER)

Component B – National Risk Assessments and National Action Plans

Specific activities will be developed further in the programme component inception phase in compliance with global efforts as well as EU processes on financial issues and in consultation with experts at CFATF, EC DG HOME and DG JUST. A preliminary list would include inter alia, and not limited to:

---

9 Including the EU list on non-cooperative tax jurisdictions
• Undertake high-level advocacy missions to solicit political support for AML/CFT programs in CARIFORUM Member States
• Organise stakeholders' sensitisation workshops on roles and responsibilities with the partnership of regional and national AML/CFT agencies
• Strengthen cooperation to guide long-term partnerships between regional governments, civil society, private sector and the international community in addressing AML/CFT gaps
• Develop implementation and action plan for operationalisation of National Risk Assessment Reports
• Assess capacity of current national data capturing mechanisms and make recommendations for necessary upgrades
• Develop or review existing templates risk mapping in engagement with the CFATF
• Carry out data collection on AML/CTF risks and prevalent predicate offences
• Write the National Risk Assessment reports
• Validate the National Risk Assessment reports with a wide range of stakeholders (organise validation workshop, conduct official adoption and approval of report)
• Design of National Action Plans which would address all outstanding deficiencies found in past Mutual Evaluations and Follow-up Reports, and refer to those legal, regulatory and institutional measures that must be put in place so that the national AML/CFT infrastructure is in keeping with all FATF Recommendations.
• Validate the National Action Plans with a wide range of stakeholders (organise validation workshop, conduct official adoption and approval of action plan)
• Support to the establishment of a strong continuous monitoring system which will oversee not only the implementation of the plans, but more generally financial compliance standards throughout the region.
• Support the implementation of the Work Plans that have been developed as result of the National Risk Assessments as well as the Improvement Plans AML/CFT System following the Fourth Round of Mutual Evaluations.

Component C – Asset Recovery and Cybercrime
Specific activities are planned to include inter alia, and not limited to:
• Review current asset recovery legislation and assess regional capacity on asset recovery to determine training strategy. This activity will benefit the work already commenced by CARICOM and the RSS Asset Recovery Unit on a Model Civil Asset Recovery Legislation as well as two regional assessments carried out by OAS and Canada.
• Design and deliver training to judicial officers towards enhancement of prosecution and judgments that facilitate asset recovery in the Region.
• Coordinate the development of dedicated Asset Recovery Units in Member States with a dedicated regional reporting structure that facilitates information sharing
• Workshop towards implementation of the Agreement for the Return and Sharing of Recovered Assets within Member States emphasising the use and strategic link between Caribbean Mutual Legal Assistance Treaty to facilitate information sharing in the promotion of the sharing of recovered assets.
• Regional stakeholder workshop of Legal and Policy Experts to identify existing legislative gaps on cybercrime at the national level in relation to already existing models
• Technical assistance to Member States regarding legislative and policy improvements/amendments with respect to anti-cybercrime legislative frameworks, including training of legislators
• Design, development and delivery of targeted trainings on cybercrime for law enforcement and judiciary professionals in Member States
• Design and develop cybercrime training modules to be included in the curricula of the regional universities and educational institutions (including regional and national police schools)
• Undertake needs analysis for the implementation of the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)
• Technical assistance to CARICOM/IMPACS as the lead implementing agency of the CCSCAP
• Design, development and delivery of training on cybercrime as it relates to information gathering and strategic analysis for The Regional Intelligence Fusion Centre (RIFC) and National Intelligence Points of Contacts in Member States.
• Undertake awareness actions targeting decision makers and parliamentarians

4.3 Intervention logic

Component A – Implementation of the Mutual Evaluation Programme

Component B – National Risk Assessments and National Action Plans

The aim of the action is to assist in strengthening the AML/CFT regimes in the CARIFORUM Member States through support at national and regional level, and through support to the CFATF, with the overall goal of increasing financial compliance in the Caribbean region.

Identifying and addressing weaknesses in the AML/CFT regimes through the National Risk Assessments and National Action Plans allow for concrete actions to be taken by Member States and their national AML/CFT agencies. Monitoring the compliance level with the FATF standards is furthermore an effective way to ensure that actions taken by national authorities are sustained and improved upon. Over time the mutual evaluation exercise conducted by the FATF and other Assessment Bodies, like the World Bank and the IMF, has proved to be a useful tool in ensuring compliance with international standards.

Component C – Asset Recovery and Cybercrime

The aim of the action is build capacity on Asset Recovery and Cybercrime issues in the region.

Efforts are underway to strengthen the CARIFORUM Member States legislation on asset recovery while also supporting regional coordination through the recent establishment of the ARIN-CARIBE network. This action aims to complement the process by the delivery of targeted trainings to build capacity of judicial officers in the region as well as support to regional coordination and information sharing on asset recovery. The rationale is that in addition to establishing legislation and coordination structures, targeted trainings and support are needed to move forward in practice.

Similarly, legislation on cybercrime has been enacted in most CARIFORUM Member States. There is a remaining need to build capacity for law enforcement and judiciary personnel in particular on
how to address and counter cybercrime in practice. To ensure sustainability of the action, the targeted trainings will also be developed as training modules to be included in the curricula of regional and national educational institutions. A review of the current state of cybercrime legislation in the region is necessary to ensure that the trainings developed are in support of legislation compliant with international standards on cybercrime (the Budapest convention). Finally, while there are regional structures in place to promote regional coordination on cybercrime, capacity is still a concern. The action will therefore seek to strengthen these regional structures (CARICOM/IMPACS and subagency RIFC) to promote coordination at the regional level as well as the implementation of the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).

5. IMPLEMENTATION

5.1 Financing agreement
In order to implement this action, it is foreseen to conclude a financing agreement with CARIFORUM, as referred to in Article 17 of Annex IV to the ACP-EU Partnership Agreement.

5.2 Indicative implementation period
The indicative operational implementation period of this action, during which the activities described in section 4.2 will be carried out and the corresponding contracts and agreements implemented, is 60 months from the date of entry into force of the financing agreement.

Extensions of the implementation period may be agreed by the Commission’s authorising officer responsible by amending this decision and the relevant contracts and agreements; such amendments to this decision constitute non-substantial amendment in the sense of Article 9(4) of Regulation (EU) No 322/2015

5.3 Implementation of the budget support component
N/A

5.4 Implementation modalities for an action under project modality

(a) Objectives of the grant, fields of intervention, priorities of the year and expected results
The specific objective of the grant is to enable the CFATF to implement the Mutual Evaluation Programme in the region. Specifically CFATF will support countries to prepare and carry out the ongoing Fourth Round of Mutual Evaluation Missions which started in January 2015 and are due to continue to 2022. Main expected outcome is to have reports produced for the global quality and consistency review process.

(b) Justification of a direct grant
Under the responsibility of the Commission’s authorising officer responsible, the recourse to an award of a grant without a call for proposals is justified as CFATF is specifically mandated by its Member States to coordinate, organise and implement the evaluation missions. CFATF has already supported three countries through the Fourth Round of Mutual Evaluation Missions (Jamaica, the
Bahamas and Trinidad and Tobago\(^{10}\)) which makes them well placed to continue carry out these activities in the region.

(c) Essential selection and award criteria

The essential selection criteria are the financial and operational capacity of the applicant.

The essential award criteria are relevance of the proposed action to the objectives of the call; design, effectiveness, feasibility, sustainability and cost-effectiveness of the action.

(d) Maximum rate of co-financing

The maximum possible rate of co-financing for this grant is 100%. In accordance with Articles 192 of Regulation (EU, Euratom) No 966/2012 applicable by virtue of Article 37 of (EU) regulation n° 323/2015 if full funding is essential for the action to be carried out, the maximum possible rate of co-financing is increased to 100%. The essentiality of full funding will be justified by the Commission’s authorising officer responsible in the award decision, in respect of the principles of equal treatment and sound financial management.

The programme will be financing a maximum of 50% of the costs of the missions, the remainder to be financed by the Member States that are to be evaluated.

(e) Indicative trimester to conclude the Grant agreement

2018 Q2.

5.4.1.1 (Bis) Grant: direct award: Component B: National Risk Assessments and National Action Plans

(a) Objectives of the grant, fields of intervention, priorities of the year and expected results

The specific objective of this grant is to strengthen financial compliance in the Caribbean region through supporting CARIFORUM Member States in carrying out National Risk Assessments as well as to design and implement National Action Plans. Additionally support will be given to Work Plans that have been developed as result of National Risk Assessments. Main expected outcome is to have increased knowledge and awareness of weaknesses in the region’s AML/CFT regimes with corresponding national action plans to address these issues.

(b) Justification of a direct grant

This component will be implemented with a Member State Agency or with an International Organisation, preferably in a consortium, in accordance with Article 58(1) (c) of Regulation (EU, Euratom) No 966/2012. This implementation is justified because of the nature of the activities foreseen (provision of capacity building and technical assistance in a highly specialised topic in accordance with the principles of rule of law) but also in order to avoid duplication and overlap with similar activities of the entities that are active in the region with relevant interventions.

(c) Eligibility conditions

EU Member States Agencies and/or International Organisations are best placed to cover the fields of expertise required to perform interventions in the areas of financial compliance, best practices for tax information exchanges, capacity building, and regional cooperation while ensuring transparency and confidentiality. A consortium would be preferable as it allows for the inclusion of

---

implementing partners providing expertise on highly specialised topics, also with context-specific expertise on financial compliance issues in the Caribbean region.

(d) Essential selection and award criteria
The essential selection criteria are the financial and operational capacity of the applicant.
The essential award criteria are relevance of the proposed action to the objectives of the call; design, effectiveness, feasibility, sustainability and cost-effectiveness of the action.

(e) Maximum rate of co-financing
The maximum possible rate of co-financing for this grant is 100%
In accordance with Articles 192 of Regulation (EU, Euratom) No 966/2012 applicable by virtue of Article 37 of (EU) regulation n° 323/2015 if full funding is essential for the action to be carried out, the maximum possible rate of co-financing is increased to 100 %. The essentiality of full funding will be justified by the Commission’s authorising officer responsible in the award decision, in respect of the principles of equal treatment and sound financial management.

(f) Indicative trimester to conclude the Grant agreement
2018 Q3

5.4.1.1. (Ter) Grant: direct award: Component C: Asset Recovery and Cybercrime, CARICOM/IMPACS

(a) Objectives of the grant, fields of intervention, priorities of the year and expected results
The specific objective of the grant is to enable CARICOM IMPACS to support capacity building in the region on asset recovery and cybercrime. Main expected outcome is to have strengthened capacity at national level in CARIFORUM Member States and greater collaboration/coordination at regional level on asset recovery and cybercrime.

(b) Justification of a direct grant
Under the responsibility of the Commission’s authorising officer responsible, the recourse to an award of a grant without a call for proposals is justified as CARICOM/IMPACS is the region’s mandated implementing agency on crime and security.

(c) Essential selection and award criteria
The essential selection criteria are the financial and operational capacity of the applicant.
The essential award criteria are relevance of the proposed action to the objectives of the call; design, effectiveness, feasibility, sustainability and cost-effectiveness of the action.

(d) Maximum rate of co-financing
The maximum possible rate of co-financing for this grant is 100%
In accordance with Articles 192 of Regulation (EU, Euratom) No 966/2012 applicable by virtue of Article 37 of (EU) regulation n° 323/2015 if full funding is essential for the action to be carried out, the maximum possible rate of co-financing is increased to 100 %. The essentiality of full funding will be justified by the Commission’s authorising officer responsible in the award decision, in respect of the principles of equal treatment and sound financial management.
(e) Indicative trimester to conclude the Grant agreement
2018 Q2.

5.4.1.2. Procurement (direct management)

<table>
<thead>
<tr>
<th>Subject</th>
<th>Type (works, supplies, services)</th>
<th>Indicative number of contracts</th>
<th>Indicative trimester of launch of the procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation and Audit</td>
<td>services</td>
<td>3</td>
<td>Q2/2020 and Q4/2022</td>
</tr>
<tr>
<td>Communication and visibility</td>
<td>services</td>
<td>1</td>
<td>Q4 2018</td>
</tr>
</tbody>
</table>

5.5 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.

The Commission’s authorising officer responsible may extend the geographical eligibility in accordance with BudgetArticle 22(1)(b) of Annex IV to the ACP-EU Partnership Agreement on the basis of urgency or of unavailability of products and services in the markets of the countries concerned, or in other duly substantiated cases where the eligibility rules would make the realisation of this action impossible or exceedingly difficult.

5.6 Indicative budget

<table>
<thead>
<tr>
<th>Programme activity</th>
<th>EU contribution (amount in EUR)</th>
<th>Indicative third party contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.1.1 Component A: Grant to CFATF Implementation of the Mutual Evaluation Programme</td>
<td>1 800 000</td>
<td>N.A.</td>
</tr>
<tr>
<td>5.4.1.1 (Bis) Component B: Pillar Assessed Grant Implementation of National Risk Assessments and Design of National Action Plans</td>
<td>4 050 000</td>
<td>N.A.</td>
</tr>
<tr>
<td>5.4.1.1 (Ter) Component C: Grant to CARICOM / IMPACS Asset Recovery and Cybercrime Asset Recovery Cybercrime</td>
<td>2 400 000</td>
<td>N.A.</td>
</tr>
<tr>
<td></td>
<td>600 000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 800 000</td>
<td></td>
</tr>
<tr>
<td>5.4.1.2 Evaluation and Audit</td>
<td>150 000</td>
<td></td>
</tr>
<tr>
<td>5.4.1.2 Communication and visibility</td>
<td>50 000</td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>8 450 000</td>
<td></td>
</tr>
</tbody>
</table>
5.7 Organisational set-up and responsibilities

Component A – Implementation of the Mutual Evaluation Programme

The implementation of this component will be coordinated and led by CFATF through a programme steering committee with a view to also promote (potentially host) yearly donor forums on AML/CFT issues in the region.

CFATF is an organisation of twenty-five (25) states (Antigua & Barbuda, Anguilla, Aruba, The Bahamas, Barbados, Belize, Bermuda, The British Virgin Islands, The Cayman Islands, Curacao, Dominica, El Salvador, Grenada, Guyana, Republic of Haiti, Jamaica, Montserrat, St. Kitts & Nevis, St. Lucia, St. Maarten, St. Vincent & The Grenadines, Suriname, The Turks & Caicos Islands, Trinidad & Tobago, and Venezuela) of the Caribbean Basin, which have agreed to implement common countermeasures to address the problem of criminal money laundering. It was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992. The meeting in Aruba convened representatives of Caribbean and Central American countries to develop a general approach to the problem of criminal proceeds, resulting in nineteen (19) recommendations. The subsequent meeting of ministers in Jamaica concluded with the Kingston Declaration which endorsed the commitment of Member States to the implementation of the nineteen (19) recommendations and further that the implementation should be coordinated through the establishment of the CFATF secretariat. The main objective of the CFATF is therefore to achieve effective implementation of and compliance with FATF recommendations to prevent and control money laundering and to combat the financing of terrorism. The Secretariat has been established as a mechanism to monitor and encourage progress to ensure full implementation of the Kingston Ministerial Declaration. The CFATF is specifically mandated by its Member States to coordinate, organise and implement the evaluation missions and as the only organisation officially assigned in CARICOM to guide such a process it is therefore in a position of de jure and de facto monopoly.

Component B: National Risk Assessments and National Action Plans:

The implementing organisation(s) would be selected for a Pillar Assessed Grant, through a process managed by the Commission in close coordination with CARIFORUM and the CFATF.

Component C: Asset Recovery and Cybercrime

CARICOM IMPACS will be the agency responsible for implementing the component and coordinating the interactions of the various agencies and partners involved including consultants as required. CARICOM IMPACS is the nerve centre of the Region’s multilateral Crime and Security management architecture, designed to administer a collective response to the crime and security priorities of CARICOM Member States. The agency is charged with primary responsibility for the implementation of the regional crime and security agenda and reports directly to the Council of Ministers Responsible for Crime and Security (CONSLE). The Agency also receives inputs and direction regarding regional security priorities through regular meetings of the Standing Committees of Commissioners of Police, Chiefs of Military, Chiefs of Immigration, Comptrollers of Customs and Heads of Intelligence and Financial Crimes and Heads of Correctional Facilities.

The agency will seek to recruit a competent Project Manager to coordinate all the activities related to Cybercrime and Asset Recovery components. The project will be executed through engagement of other critical stakeholders such as the Caribbean Telecommunications Union (CTU) and the Organisation of American States (OAS/CICTE), the Regional Security System including the Asset
Recovery Unit (RSS ARU), the Caribbean Financial Action Task Force (CFATF) as well as in collaboration with CARIFORUM Member States, international organisations and third state partners with whom we have established relationships with such as formal Memorandums of Understanding. These include the United Nations and its agencies, United Kingdom (UK), United States (US) to facilitate the capacity building aspects of the programmes and technical expertise required.

IMPACS technical staff will assist the Project Unit (consisting of a Project Manager and a Project Assistant) with the interactions with the technical expertise required from our partner agencies. There will be two oversight committees for the two components comprising of key stakeholders to guide and assess activities – one for asset recovery and one for cybercrime.

5.8 Performance monitoring and reporting

The day-to-day technical and financial monitoring of the implementation of these actions will be a continuous process and part of the implementing partners’ responsibilities. To this aim, the implementing partners shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its results (outputs and direct outcomes) as measured by corresponding indicators, using as reference the logframe matrix. Particular attention shall be given from the outset to the logframe matrix which will be updated at the start of the implementation to include baseline data and corresponding indicators, including gender disaggregated data where applicable. The structure of the Monitoring and Evaluation system of each Component shall be elaborated on the basis of these parameters prior to the start of the implementation with clear indication of the reporting responsibilities and adequate allocation of human and financial resources to follow up. The reporting shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the budget details for the action. The final report, narrative and financial, will cover the entire period of the action implementation.

In addition to the reporting requirements in accordance with implementing contracts, Implementing Agencies for components A, B and C shall submit timely reports to the Regional Authorising Officer (RAO) of CARIFORUM.

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).

5.9 Evaluation

Having regard to the importance of the action, a mid-term and a final evaluation will be carried out for this action or its components via independent consultants contracted by the Commission.

The mid-term evaluation will be carried out for problem solving and learning purposes, in particular with respect to ensuring that sufficient progress is being made with the capacity building activities under the three components.

The final evaluation will be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the fact that the action is aimed at strengthening the region’s compliance with FATF recommendations as well as the capacity of the region (at regional as well as national level) to counter cybercrime.
The Commission shall inform the implementing partners at least 1 month in advance of the dates foreseen for the evaluation missions. The implementing partners shall collaborate efficiently and effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities.

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

Indicatively, two contracts for evaluation services shall be concluded under Framework contract in months 33 and 66 of the project.

5.10 Audit

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 audits or expenditure verification assignments for one or several contracts or agreements.

Indicatively, one contract for audit services shall be concluded under a framework contract in month 66 of the project.

5.11 Communication and visibility

Communication and visibility of the EU is a legal obligation for all external actions funded by the EU.

This action shall contain communication and visibility measures which shall be based on a specific Communication and Visibility Plan of the Action, to be elaborated at the start of implementation and supported with the budget indicated in section 5.6 above.

In terms of legal obligations on communication and visibility, the measures shall be implemented by the Commission, the partner country, contractors, grant beneficiaries and/or entrusted entities. Appropriate contractual obligations shall be included in, respectively, the financing agreement, procurement and grant contracts, and delegation agreements.

The Communication and Visibility Manual for European Union External Action shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations.