Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

D1.1 Project Management Handbook

WP number and title	WP1 – Project Management
Deliverable number	D1.1
Version Number	1.0
Document Reference	Project Management Handbook
Lead Beneficiary	AIT
Deliverable type	R
Planned deliverable date	2022-01-31
Date of Issue	2022-01-31
Dissemination level	PU
Authors	AIT
Contributor(s)	IANUS
Keywords	Project management, consortium, coordination, quality plan, workplan

This project has received funding from the European Union's ISFP-2020-AG-TERFIN program under the Grant Agreement No. 101036262

Document History

Version	Date	Status	Author(s), Reviewer	Description
V0.1	2022-01-26	Draft	AIT	First draft
V0.2	2022-01-28	Draft	AIT, IANUS	Updated version integrating review comments
V1.0	2022-01-31	Final	AIT, IANUS	Final version

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of the Document

This report focuses on providing Anti-FinTer's consortium partners with a complete and efficient commonly shared operational methodology, and a set of management rules and guidelines to be adopted in order to manage and carry out the activities and fulfil the contractual obligation towards the European Commission, reducing the overhead and increasing the efficiency and quality of the work carried out.

The document aims to provide:

- **procedures, rules, standards** and **best practices** to be adopted in Anti-FinTer for the complete management of processes;
- **templates** to produce high-quality deliverables and reports for the Anti-FinTer project including a standard format for meeting organisation and reports;
- explanation of the tools used in the project to facilitate online collaboration and providing a shared space, including a project repository dedicated to exchange documents;
- **process to make sure that contents** and presentation of all deliverables produced in Anti-FinTer **are consistent**;
- a list of rules to ease the **flow for an effective communication and collaboration** between partners as well as for external communication and dissemination of a project results (i.e. the procedures for meetings, for progress reporting, etc.);

Moreover, in the document the **management structures**, which have been established in Anti-FinTer to effectively manage and address the different aspects of the project, are described.

1.2 Scope and Intended Audience

This deliverable focuses on providing the Anti-FinTer partners with explanation of rules and guidelines to be adopted in the project for the complete management of processes. These instruments will be oriented to the successful achievement of all activities of the Anti-FinTer project, in order to fulfil the contractual obligations towards the European Commission.

1.3 Structure of the Document

The deliverable is structured as reported below:

Chapter 2 – Project Overview – A summary of Anti-FinTer's main concept and objectives.

Chapter 3 – Anti-FinTer Organization – Anti-FinTer's consortium is presented in this chapter, with a description of each partner and related operational team involved in the project. In addition, this chapter provides also an overview about the internal structure and its operational bodies.

Chapter 4 – Activity Organization, Control and Monitoring – This chapter provides a description of the work organization within Anti-FinTer, the work breakdown structure and methodology. In addition, it provides also some instruments that will be set up during the project development in order to assess project advances. Description of procedures to follow in order set up project meetings is presented here too.

Chapter 5 – Risk Management and **Quality Assurance** – Overview of actions that will be handled to prevent risks and mitigate their impact on project activities and results and a description of quality assurance goals that will be treated in detail in D1.2 (M3).

1.4 Related Deliverables

The following deliverables are highly relevant to the project execution and should also be considered as extensions of the Project Handbook:

D1.2 Quality Assurance Plan (M3): The Quality Assurance Plan details the quality plan for internal and external communication, software development and document management, including: deliverable and milestone management, document structure, file naming and version control, and the deliverable production and review workflow.

D1.3 Ethical Requirements and Code of Conduct (M3): This report will define the project internal guidelines necessary to ensure that the consortium pays appropriate attention to the effects of the project on individual rights and freedoms (e.g., data protection and privacy), and that consortium actions comply with all relevant ethical principles and all applicable international, EU and national law on ethical issues while carrying out the project.

D5.1 Dissemination, Communication and Outreach plan (M3): This plan describes the communication methods, target groups, and messages as well as the list of planned Dissemination activities.

2 Project Overview

Anti-FinTer will improve law enforcement capabilities, increase capacity and develop expertise in the area of terrorist financing associated with activities in the Dark Web, crypto-assets, new payment systems and darknet marketplaces. To maximize its impact and long-term sustainability of the project outcomes, particular attention will be given to establishing a long-term Public-Private Partnership (PPP) initiative through the involved partners' connections (the EACTDA association, ENLETS , UN-OICT , I-LEAD and related networks). Improvements will be brought about by three distinct actions:

1. Facilitation of knowledge exchange among stakeholders and the documentation of best practices, risk analysis and policy recommendations in four workshops and multiple virtual meetings;
2. Integration of existing TRL6+ tools (e.g., GraphSense , Dark Web Monitor) to create a Toolkit for training investigators and analysts in new investigative techniques that include crypto-asset analysis, new payment channels such as the Lightning Network , text and image analysis from surface web, dark web and social media channels to identify common actors and correlate terrorist activity with cryptocurrency transactions, and artificial intelligence analytics for detecting transaction anomalies;
3. Development of training curricula and an exercise environment used in two virtual and three face-to-face training events that will be organized and carried out during the project along with two train-the-trainer events that will ensure a wider impact for the curricula, which will be made available afterwards through organizations such as Europol, CEPOL and FRONTEX.

- **Project Acronym:** Anti-FinTer
- **Full Project Name:** Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism
- **Funding Program:** ISFP-2020-AG-TERFIN
- **Topic:** Countering terrorist financing focusing on the cooperation of public and private actors and emerging technologies
- **Duration:** 2 Years (January 2022 – December 2023)
- **Consortium:** 10 Partners
- **Budget:** 1.497 M€ Financing: 1.348 M€ (90%)

2.1 Objectives and KPIs

To achieve the general goal of improving law enforcement capacity and developing expertise in terrorist financing investigations, the Anti-FinTer project has defined the following eight Specific Objectives (SO) and associated Key Performance Indicators (KPI):

2.1.1 (SO1) Knowledge transfer and capacity building for the stakeholders (LEAs/FIUs)

Stakeholders will be kept up to date with current technological tools to collect intelligence and subsequently to combat the phenomenon. This will include the creation of a Knowledge Hub with broad multi-disciplinary participation, including PPPs, to serve as a long-term enabling factor to keep up with the developments in this field and to introduce appropriate solutions.

KPIs

- 20 virtual Stakeholder Roundtable meetings held by the end of the project
- 50 hub participants subscribed by the end of the project
- Members of 25 distinct European public security organizations and/or PPPs participating in the Knowledge Hub

2.1.2 (SO2) Exploration and documentation of new investigative methods for terrorist financing cases

Continual Stakeholder Roundtable meetings with Knowledge Hub participants (with an emphasis on the aforementioned "parallel investigations" and "follow the actor" concepts) will be organised. This knowledge exchange will result in a report on the terrorist financing modi operandi made possible through cryptocurrency, (Dark) Web and darknet transactions, and the investigative practices to counter these operations.

KPIs

- Identification and reporting of new investigative methods available in M8 of the project
- Four IOCTA terrorism financing use cases analysed in the investigative methods report

2.1.3 (SO3) Provision of a risk assessment report

The risk assessment report will map current and future terrorist financial risks and current state of play of LEAs capacity to address current and emerging threats and policy recommendations for the EU and LEA stakeholders.

KPIs

- Risk Assessment and Policy Recommendations report available by M24 of the project

2.1.4 (SO4) Provision of relevant datasets

The datasets will include: transaction data from at least four different cryptocurrencies; historical data from at least four different dark web markets, and more than ten-thousand images from dark web markets.

KPIs

- At least three datasets as described above provided to EACTDA by the end of the project

2.1.5 (SO5) Provision of an integrated Toolkit

The toolkit will include high TRL-level results from projects such as ASGARD, TITANIUM, DANTE, and TRUSTS for a) virtual currency analysis for tracing money laundering and illicit sales, b) dark web analysis of funding activities in darknet markets, c) visual analytics for identifying illicit goods in darknet markets, and d) artificial intelligence analytics for detecting transaction anomalies.

KPIs

- Toolkit ready for stakeholder evaluation by M8 of the project
- Four tools (defined in Activity 3.2) available to practitioners for evaluation by M16 of the project
- At least three tools provided to EACTDA at the end of the project

2.1.6 (SO6) Definition of training curricula technologies and the organization of online and face-to-face training events

The training events will be organized during the project. Curricula will be made available afterwards through international organizations such as Europol, CEPOL, FRONTEX and the United Nations.

KPIs

- 140 training person-days (20 participants in three face-to-face training events, 30 participants in two online training events, 20 participants in two train-the-trainer events)
- Participants from 20 distinct European public security organizations and more than 15 EU member states registered for training events

2.1.7 (SO7) Development of an environment for joint exercises of and organisation of Hackathons

The environment will allow stakeholders to use and evaluate the Anti-FinTer Toolkit. These exercises will be designed as a Capture-the-Flag information security competition that challenges user to solve a variety of tasks related to terrorist financing investigations.

KPIs

- 60 Hackathon participants (20 participants in three face-to-face Hackathon events)
- Exercise environment and training exercises provided to EACTDA at the end of the project

2.1.8 (SO8) Organisation of dissemination and outreach activities

The goal is to encourage dialogue among the individual project beneficiaries and between the community of project beneficiaries, stakeholders and the Commission services and promote more interaction about innovation in project outputs and to increase visibility, learning effects and synergies.

KPIs

- Four outreach events (2 webinars, 2 seminars) with at least 220 participants (60 participants per webinar, 50 participants per seminar)

2.2 Activities

The project activities are structured in four main pillars. The first one will focus on extending the current well-established “follow the money” financial investigation approach, by a) adopting the concept of “parallel financial investigations” (as introduced by FATF) that refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation and b) introducing a novel “follow the actor” approach, i.e. a methodology that will put the focus on jointly analysing multiple financial investigations/cases, to reveal the identities of the same (group of) actors that are behind all these incidents (D2.1, M8).

In parallel, as the second pillar, the project will be developing the Toolkit and training environment to host all project analytical/investigative tools and the online platforms to support the subsequent training activities. The plan is to have this infrastructure ready for use by M12 (D3.3), in time for the execution of joint exercises in M18 and M23.

The third pillar consists of training and joint exercises constitute the third project pillar, which will be conducted through Capture the Flag (CtF) exercises that make use of the project Toolkit and are extensively used in other domains (e.g. military) in a distributed environment with the support of project technical partners. In addition, we will employ the Hackathon methodology was pioneered by the ASGARD project and was considered highly useful by LEA participants. This approach enables instant feedback and an agile development approach that combines hands-on testing and requirements engineering during an intensive face-to-face event between stakeholders and developers. Hackathons supplement but do not replace regular training events; in addition, the project plans two "train-the-trainer" events, two online-training sessions, and three technical training sessions that precede each Hackathon to ensure the effectiveness of the Hackathon sessions.

The final pillar consists of two horizontal activities, namely the Coordination of the project and the Dissemination and Communication activities. Project outcomes, policy recommendations and briefs will be distributed at the national, regional and EU levels also via the organisation of two (2) European Seminars (physical) and two (2) webinars (virtual), and the implementation of the project Knowledge Hub and associated stakeholder meetings.

Dissemination and outreach activities are planned to encourage dialogue among the individual project beneficiaries and between the community of beneficiaries, stakeholders and the Commission services and promote more interaction about project outputs and innovations, thus increasing visibility, learning effects and synergies. The project also designs to deliver two Webinar sessions and two seminars with the participation of external experts and stakeholders.

2.3 Stakeholders

Short-term beneficiaries of the Anti-FinTer project outputs include the four LEA stakeholders that are directly involved in the project (AEAT, MJPJ, FCIS, GDCOC). In the medium term, the pool of beneficiaries expands to stakeholders that participate in the project Knowledge Hub and training exercises. In the long term, beneficiaries will include all European stakeholders that have access to the training materials and tools curated by EACTDA, as well as world-wide users of the United Nation's data analytics platform.

Anti-FinTer will bring together a rich panel of practitioners from EU national authorities to identify new trends related to crypto-assets, new payment methods and crowdfunding used by terrorists and to adapt them in their operational pipeline. The project has received Letters of Support from several stakeholder organizations that will provide an initial panel of practitioners that will participate in projects activities, in context of the Knowledge Hub in WP2 and the Webinar series in WP5.

For example, the project will engage the ENLETS Technology Interest Group on Financial Crime that is also related to terrorism financing. Through the cooperation with UN-OICT, Financial Intelligence Units worldwide will also be invited to participate in the practitioner group. Our support of EACTDA (an engagement with EACTDA through four project partners who are members) enables direct access to additional LEA and forensic stakeholders. Finally, the support of I-LEAD will connect us with practitioners through dissemination events and workshops. Thus, not only will the project start with a rich panel of experts committed through the LoS, but the prospects for growing this panel through organizational contacts are very good.

3 Anti-FinTer Organization

3.1 Anti-FinTer Consortium

In Anti-FinTer we follow a multidisciplinary approach with a consortium structure consisting of public organisations, security experts, criminology scientists, social sciences, training experts, research and technology organisations specialized in security research, and SMEs. More specifically, Anti-FinTer consortium is composed of 4 public organisations (FCIS, AEAT, MJPJ, and GDCOC) 1 University (ULIM), 3 research centres (AIT, FORTH, and VICOM), and 2 SMEs specialised in security (IANUS and CFLW).

- **AIT** (AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH) is the largest RTO in Austria and its Center for Digital Safety & Security (DSS) has extensive experience in the research and development of ICT technologies for cybersecurity, forensics, and law enforcement applications, in particular through the development of the open-source crypto-asset forensics platform GraphSense. Furthermore, DSS has a long track record in the coordination and management of national and international projects in this area (e.g., TITANIUM) and is thus suited for the coordinator role.
- **FORTH** (IDRYMA TECHNOLOGIAS KAI EREVNAS) is the largest RTO in Greece, with significant experience in European secure society calls. Their Human Computer Interaction (HCI) laboratory brings key expertise in Big Data and Artificial Intelligence analytics to the forensic applications in the project.
- **VICOM** (FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUALY COMUNICACIONES VICOMTECH) has a similar position in Spain, working closely with national and international LEA stakeholders and participating in multiple secure societies projects (e.g., GRACE, AIDA, CAPER and ASGARD as coordinator). VICOM is also the founder and the first President of the European Anti Cybercrime Technology Development Association (EACTDA).
- **CFLW** (CFLW CYBER STRATEGIES BV) is the newly established curator and developer of the Dark Web Monitor tool and, through its founder Mark van Staalduinen, brings years of experience and collaboration with LEAs in darknet investigations.
- **ULIM** (UNIVERSITY OF LIMERICK) provides expertise in data ethics as well as the experience and infrastructure for LEA training through their long-standing collaboration with the Irish National Center for Taxation Studies.
- **IANUS** (IANUS CONSULTING LTD) is a Cypriot SME that brings years of experience of their Staff in international security-related programs, together with a wide network of European contacts. IANUS also brings successful experience with ISFP projects and related communication and dissemination activities.
- The four **LEA partners** have been chosen to represent geographically diverse European states and law enforcement roles including
    - Tax authorities (**AEAT**: AGENCIA ESTATAL DE ADMINISTRACION TRIBUTARIA, Spain)
    - FIUs (**FCIS:** FINANSINIU NUSIKALTIMU TYRIMO TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS, Lithuania; and **MJPJ:** MINISTÉRIO DA JUSTIÇA, Portugal), and
    - Organized crime units (**GDCOC:** GLAVNA DIREKTSIA BORBA SORGANIZIRANATA PRESTUPNOST, Bulgaria).

3.2 Team

AIT leads WP1 (Role: Project Coordinator), and also contribute their expertise in crypto-asset forensics through the integration of their open-source GraphSense platform in **WP3** and to the development of associated training curricula and exercises in **WP4**.

CFLW leads WP2 (Role: Innovation Manager), gathering requirements, organizing the Knowledge Hub and exchange of best practices among LEA stakeholders within the project, associated stakeholders, and wider European networks, as well as contribute to the integration of darknet forensics tools through the Dark Web Monitor in **WP3** and to the development of associated training curricula and exercises in **WP4**.

FORTH leads WP3 (Role: Technical Manager), managing the customization of the forensic tools and their integration as the project Toolkit, including their own big data and image analysis technology for identifying marketplaces and transactions related to terrorist organizations and financing in darknet markets and related open-source intelligence sources.

VICOM leads WP4 (Role: Training Manager), applying the methodologies established in the ASGARD project to establish and organize training exercises. VICOM also integrates AI-based financial transaction anomaly detection algorithms with forensic tools in the context of **WP3**.

ULIM contributes training facilities and expertise to WP4, helping to define and deliver training curricula to LEA stakeholders and define and implement the train-the-trainer program. ULIM also carries out the project SELP analysis for **WP1 Activity 1.3**.

IANUS leads WP5 (Role: Dissemination Manager) and organizes the associated activities around communication, dissemination and outreach with stakeholders and PPPs throughout Europe.

The four LEA partners (**AEAT, MJPJ, FCIS, GDCOC**) contribute to requirements and the exchange of best practices through **participation in the Knowledge Hub in WP2**. These partners also participate in training and provide feedback on tools through exercises in **WP4** and contribute to outreach events in **WP5**.

Participant No	Participant organisation name	Short Name	Country
1	AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AIT	Austria
2	IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	Greece
3	FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUALY COMUNICACIONES VICOMTECH	VICOM	Spain
4	IANUS CONSULTING LTD	IANUS	Cyprus
5	CFLW CYBER STRATEGIES BV	CFLW	Netherlands
6	UNIVERSITY OF LIMERICK	ULIM	Ireland
7	FINANSINIU NUSIKALTIMU TYRIMO TARNYBA PRIE VIDAUS REIKALU MINISTERIJOS	FCIS	Lithuania
8	AGENCIA ESTATAL DE ADMINISTRACION TRIBUTARIA	AEAT	Spain
9	MINISTÉRIO DA JUSTIÇA	MJPJ	Portugal
10	GLAVNA DIREKTSIA BORBA SORGANIZIRANATA PRESTUPNOST	GDCOC	Bulgaria

Table 1: Anti-FinTer Consortium Partners (Project Beneficiaries)

3.3 Project Structure and Management Boards

3.3.1 Overall management structure

Anti-FinTer is managed overall in accordance with standard Project Management and Risk Management best practices. The granularity of the management structure (refer to Figure 1) has been chosen based on the size,

duration, and complexity of the project. This is based in part on AIT's experience in coordinating projects ranging in budget from 300 thousand Euros to 12 million Euros. TITANIUM falls in the middle of this spectrum. The project's volume, as well as its international aspect, demands a separation between implementation (carried out by students, researchers, and developers), which is managed by the Executive Board, and governance (carried out by professors, managers, and other higher-level decision makers), which is carried out by the General Assembly.

By the appointment of a series hierarchical management boards, from the General Assembly, which maintains overall control of the Project at a strategic level on behalf of the Consortium Member Organisations, through the Executive Board and then down to Work Package Leads who are responsible for their own deliverables, it is possible to monitor and direct the overall programme flexibly at both micro- and macro-level, with all decisions taken at the appropriate level of authority.

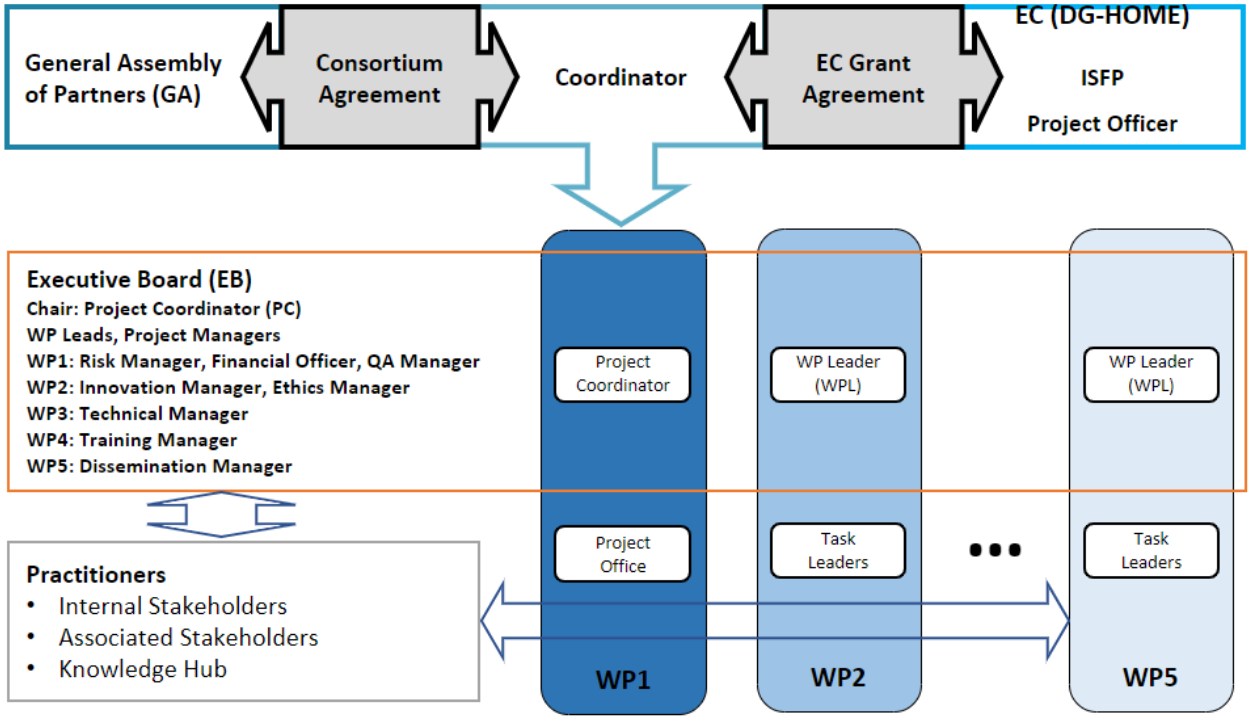

Figure 1 Project Governance Structure

3.3.2 Project Management

Project Coordinator (AIT): The main role of the PC is the overall administrative management of the project, being the single point of contact with the European Commission (EC). The PC co-ordinates all the communication channels within all the Partners to ensure progress and quality in the work and provides the EC with technical, managerial, and financial information. He chairs the General Assembly (GA) and will closely interact with all other project key project functions.

Project Office (AIT): Members of the Project Office provide full organisational and administrative support to the project team and to ensure the smooth running of the department operations, take minutes of meeting and maintain records for the operations and project team, develop and maintain document control processes for the efficient management of the project.

Financial Officer (AIT): The main roles of the FO are to supervise the distribution of EC payments to Partners, preparation of the reports, cost statements and project documents required by the EC.

3.3.3 WP Leaders

The main role of the WPL (AIT, CFLW, FORTH, VICOM, IANUS) are to participate in the Project management team, to coordinate all activities with the WP, to identify and report possible risk areas and risks and to report on the progress and the use of resources within the WP.

3.3.4 General Assembly

The General Assembly (GA) must ensure that the project functions properly. The General Assembly decides on matters relating to budget, work plan, partner performance, alteration of the Consortium Agreement (CA), or premature project termination. Voting rules will be defined in the CA. The GA is composed of one Principal representative from each partner. This Principal must have the legal authority, or power of attorney, to make binding decisions on behalf of the entity they represent. The Project Coordinator (PC) is the Chair of the GA. This body meets infrequently, but extraordinary meetings may be called by the Chair whenever necessary.

3.3.5 Executive Board

The PC will supervise and rely on the support of an Executive Board (EB). The EB is composed of the PC (chair) and all WP Leaders. All task Leaders will also be invited to participate in EB meetings. The EB will be responsible for the day-to-day management of the project and will report to the GA. The EB will meet regularly, typically through teleconferences every two weeks. On top of this, the project is planning four face-to-face meetings with the participation of all project partners to ensure a high degree of compliance with the planned timelines and objectives.

3.4 Roles and Responsibilities

3.4.1 Technical Manager

The main role of the Technical Manager (FORTH) is to coordinate all development and integration efforts of the project by defining development and testing cycles and to ensure the functionality and efficiency of all technical tools. The TC shall participate in all Project Management Team (PMT) meetings.

3.4.2 Innovation Manager

The role of the Innovation Manager (CFLW) is to coordinate inputs from the stakeholder community to document new investigative techniques and policy recommendations, and to organise and facilitate the project Knowledge Hub.

3.4.3 Ethics Manager

The main roles of the Ethics Manager (ULIM) are to coordinate and ensure that the ethics requirements for all Partners comply with national legislation, regulations and ethical and data protection rules in the countries where the action will be carried out.

3.4.4 Dissemination Manager

The main roles of the Dissemination Manager (IANUS) are to issue the Dissemination and Communication Plan and to coordinate all project dissemination and communications activities in close collaboration with all WP leaders and the project Coordinator.

3.4.5 Risk Manager

The main role of the Risk Manager (AIT) is to define the project risk management plan, work closely with the WPLs and the PC for the early identification of project implementation risks and the mitigation measures to be applied.

3.4.6 Quality Assurance Manager

Quality assurance managers (AIT, FORTH) define the project quality measures and set up the rules and roles so that project activities and outcomes are delivered with the highest quality.

3.4.7 Training Manager

The Training Manager (VICOM) will coordinate the definition of the training curricula, the definition of the exercises, and the planning and the execution of the project training program.

3.4.8 Trainer

Trainers (ULIM, all partners) define training curricula and carry out training. ULIM in particular will play a leading role here through the train-the-trainers program.

3.4.9 Researcher

The main role of the project researchers (all partners) is to conduct the assigned research and activities within his/her area of expertise within the approved timelines and allocated budget. The researcher regularly reports the progress to the respective task leader.

3.4.10 Law Enforcement Expert

The role of the law enforcement expert (FCIS, AEAT, MJPJ, GDCOC) – e.g., a police officer or analyst – is to provide expertise and best practices and contribute to the project Knowledge Hub, to evaluate the Toolkit through the project Hackathons, and to participate in the project train-the-trainer and training events. LEA practitioners from the four stakeholder partners will contribute specifically to Task 2.1 by discussing their experiences and best practices in the context of monthly Knowledge Hub meetings. This information will further be documented by said practitioners and contributed to the knowledge base stored and made available through the Knowledge Hub infrastructure in Task 2.3. Practitioners will also participate in Hackathons and joint exercises in the context of Task 4.3, and in the evaluation of project tools in Task 4.4. These activities involve intensive, on-going exchanges with tool developers throughout the continuous development process.

4 Activity Organization, Control and Monitoring

4.1 Work Organization

4.1.1 Work Breakdown Structure

The project's organisation regarding the overall work spread and allocation is based on a systematic approach: everything produced throughout and by the project corresponds to a Work Package task. The work division will therefore be articulated on a two-level basis:

- Level 1: Work Packages that gather group of single activities (or tasks), all with the same assigned objective. Each Work Package carries out its tasks, has autonomous control over internal issues and delivers research and development results in accordance with the Project Work Programme and within the allocated budget.
- Level 2: Single Activities, embedded within the Work Packages, which are linked to a sole and defined action, like the production of a Deliverable or demonstrator.

4.1.2 Project Plan and Work Packages

The Anti-FinTer project is organized under 5 work packages (WP) each providing one or more specific main outputs, contributing to either the macro-areas of the project scope or other supporting activities (such as quality management and control, project management, dissemination and exploitation, and so forth).

WP1 – Management and Coordination of the Action deals with all activities related to the general management and coordination of the action and all cross-cutting activities. WP1 takes care of the coordination and general management of the project, putting special attention to communication, time, cost, risk, and quality aspects. Another objective of WP1 is to address ethical and data privacy issues related to the project activities.

WP2 – Capacity Building and Knowledge Exchange includes the creation of the Knowledge Hub and supports its knowledge products with multi-disciplinary participation to serve as a long-term enabling factor supported by EACTDA to keep up with the developments in this particular field and to introduce appropriate solutions, beyond the lifetime of the project.

WP3 – Toolkit Integration and Customization creates a forensic Toolkit that will enable the familiarization, execution, experimentation and evaluation of key technological solutions related to the unravelling of terrorist financing activities on the Web (with particular emphasis on analysing Dark Web related acts). In particular, the WP will target the deployment of a set of advanced investigative and intelligence forensic tools (covering the whole operational pipeline of a corresponding cybercrime investigation study) and the provision to the practitioners of secure access to the tools within a sandbox environment that includes provisioned datasets.

WP4 – Training Curricula and Exercises i) develops training methodology and curricula for the collection and analysis of near real-time intelligence related to terrorist financing, and ii) defines and implements joint exercises for cross-border operations in the means of Hackathons. This is realized with the means of exercises by making use of the Toolkit developed within WP3 with innovative tools of high Technology Readiness Level (TRL) from previous and ongoing EU funded research projects (e.g., GraphSense, Dark Web Monitor). In Anti-FinTer we are planning three (3) Hackathon events and seven (7) training sessions.

WP5 – Dissemination, Communication and Outreach develops interaction between the project and relevant stakeholders, including National Authorities and European Institutions, and the public. The dissemination activities also include the preparation of relevant material (e.g., updated multimedia, presentations, electronic and printed brochures, factsheets, press releases). To maximise publicity and connect with practitioners and policy-makers we form and implement a project forum to serve both as a means for

exploitation and seek for opportunities for project sustainability at any level (National, Regional, European, and International). All project partners are involved in these activities.

	MONTHS																							
Number and name of the activity	**M 1**	**M 2**	**M 3**	**M 4**	**M 5**	**M 6**	**M 7**	**M 8**	**M 9**	**M 10**	**M 11**	**M 12**	**M 13**	**M 14**	**M 15**	**M 16**	**M 17**	**M 18**	**M 19**	**M 20**	**M 21**	**M 22**	**M 23**	**M 24**
WP1: Management and Coordination of the Action																								
1.1: Project management and administration (AIT)	D1.1																							
1.2: Risk management and quality assurance (AIT)			D1.2																					
1.3: SELP - Social, Ethical, Legal and Privacy factors (ULIM)			D1.3																					D1.4
1.4: Project meetings and reporting (AIT)													D1.5											D1.6
WP2: Capacity Building and Knowledge Exchange																								
2.1: Modus operandi and investigative techniques (CFLW)								D2.1																
2.2: Capacity building and policy recommendations (ULIM)																D2.2								D2.3
2.3: Knowledge Hub (IANUS)						D2.4																		D2.5
WP3: Toolkit Integration and Customization																								
3.1: Datasets formation (CFLW)												D3.1												
3.2: Tools customization (AIT)								D3.2								D3.3							D3.4	
3.3: Toolkit integration (FORTH)												D3.5												D3.6
WP4: Training Curricula and Exercises																								
4.1: Training and joint exercises planning (ULIM)			D4.1			D4.2																		
4.2: Training modules development and execution (ULIM)							D4.3																	D4.4
4.3: Joint exercises development and execution (VICOM)							D4.5																	D4.6
4.4: Evaluation and reporting (VICOM)				D4.7									D4.8											D4.9
WP5: Dissemination, Communication and Outreach																								
5.1: Dissemination and communication planning and activities (IANUS)			D5.1										D5.2											D5.3
5.2: Web site, collaboration tools and social media (IANUS)			D5.4																					
5.3: Production and distribution of dissemination materials (IANUS)						D5.5																		
5.4: Organisation of webinars and seminars (IANUS)													D5.6											D5.7

Figure 2 Anti-FinTer GANNT Chart

#	Title	Lead Partner
WP1	**Management and Coordination of the Action**	**AIT**
A1.1	Project Management and Administration	AIT
A1.2	Risk Management and Quality Assurance	AIT
A1.3	SELP – Societal, Ethical, Legal and Privacy Factors	ULIM
A1.4	Project Meetings & Reporting	AIT
WP2	**Capacity Building and Knowledge Exchange**	**CFLW**
A2.1	Modi operandi and investigative techniques	CFLW
A2.2	Capacity building and policy recommendations	ULIM
A2.3	Knowledge Hub	IANUS
WP3	**Toolkit Integration and Customization**	**FORTH**
A3.1	Datasets formation	CFLW
A3.2	Tools customization	AIT
A3.3	Toolkit integration	FORTH
WP4	**Training Curricula and Exercises**	**VICOM**
A4.1	Training and joint exercises planning	ULIM
A4.2	Training modules development and execution	ULIM
A4.3	Joint exercises development and execution	VICOM
A4.4	Evaluation and reporting	VICOM
WP5	**Dissemination, Communication and Outreach**	**IANUS**
A5.1	Dissemination and communication planning and activities	IANUS
A5.2	Anti-FinTer web site, collaboration tools and social media	IANUS
A5.3	Production and distribution of dissemination materials	IANUS
A5.4	Organisation of webinars and seminars	IANUS

Table 2: Anti-FinTer Work Breakdown Structure

4.2 Monitoring and Reporting

Project monitoring and reporting will be performed by means of:

- Periodic progress meeting;
- Periodic progress reporting;
- Review of main project milestones;

Reporting will be carried out:

- Internal Reports
- Periodic Reports, which in turn consist of
- Technical Reports
- Financial Reports

The Mid-term progress report is planned in Month 13 (D1.5).

The Periodic Progress Report to the EC is required in Month 24, while internal periodic progress reports are planned every 6 months.

4.2.1 Internal Reports

Because the official periodic report is only due at the end of the project, we must establish internal reporting at a more granular time scale in order to be able to properly manage the project and react to changes and

deviations from the project plan. The Project Office therefore requires Internal Reports that must be delivered by each partner to the coordinator every six months. These reports consist of Narrative Reports, Effort Reports and Expenditure Reports.

Narrative Reports

Narrative Reports should include information (per work package) on:

- Objectives in the period and progress towards those objectives
- Results, Milestones, Deliverables in the period
- Problems, risks, gaps, and corrective actions

The template for the Activity Report is available on the Redmine.

Effort Reports

Effort Reports should be extracted from institutional Time Sheets and detail the effort delivered for each Work Package measured in hours. Templates for Time Sheets are provided on the Redmine site.

Expenditure Reports

Expenditure Reports should include information (per work package) on:

- Estimated personnel costs
- Travel costs
- Other costs (subcontracting, publishing, material costs, etc.)

4.2.2 Periodic Reports

Periodic Progress Reports (PPRs) must be produced at M13 (deliverable D1.5 "Midterm project report) and within 60 days after the end of the project M24 (final report through the EC online system). The template for the PPR will be made available on the Anti-FinTer internal website. The PPRs will have the following structure:

- Explanation of the work carried out by beneficiaries and Overview of the progress
  - Objectives
  - Explanation of the work carried per WP
    - Work Package 1 – Management and Coordination of the Action
    - Work Package 2 – Communication, Dissemination and Community Building
    - Work Package 3 – European Operation Centers Cross Border Communication
    - Work Package 4 – Technology for Public Protection by Operation Centers
    - Work Package 5 – Training & validation including (CBRN-E) attacks
  - Impact
- Update of the plan for exploitation and dissemination of result (if applicable)
- Use of resources
  - Unforeseen subcontracting (if applicable)
  - Unforeseen use of in kind contribution from third party against payment or free of charges (if applicable)

Table 3: Reporting Period Content and Structure

Periodic Progress will include:

- Activities progress;

- Deliverables and milestones;
- Publications (Authors, title, publication, date);
- Conferences and presentations (Date, location, participants, subject, outcome).
- Effort on each Work package (PMs per WPs and months);
- Meetings (Date, location, subject, attendees);
- Travelling (Date, location, reason to travel, name of the traveller).

Progress reports will also contain the following information:

- a management-level overview of the activities carried out;
- a description of progress toward the objectives;
- a description of progress toward the deliverables foreseen;
- problems encountered during the project and actions taken to correct them.

The Coordinator will be in charge of preparing this and will ask each partner for any additional contributions.

For internal monitoring purpose, **internal periodic progress reports** shall be produced. **Every 6 months** partners will be asked by the Coordinator to report both on the progress of the project activities per WP and on the effort spent per activity in the current period. The template for the internal reports will be made available on the Anti-FinTer internal website.

In particular,

a) A **Work Package status report** will be produced by each WP leader with the following information:
   - Activities completed during the period
   - Activities in progress
   - Planned activities for the next months
   - Risks management update
   - Open issues
   - WP Meetings/conference calls
   - Publication of articles

To this goal, the WP Leaders should in turn ask Task leaders to provide their individual contributions.

b) An **Effort report** will be produced by each partner with the following information:
   - per-Task effort expenditure for the current period
   - Updates to the provisional numbers of the previous period, if any
   - Rationale for any significant deviation with respect to the planned expenditure

4.2.3 Project Deliverables

Official Deliverables and Tasks are those that are described in the Description of Work. Official deliverables need to be submitted and approved by the EC. These external constraints and goals are part of the Grant Agreement and therefore need to be met. Any discrepancy between actual and planned achievements needs to be explained and justified. Official deliverables and milestones will go through thorough quality control by peer review before being published. This process will be detailed in D1.2 “Quality Assurance Plan.”

4.3 Change Management Procedure

Amendments of the Grant Agreement become necessary for any significant change. An amendment is necessary for 1) adding a new beneficiary; 2) change of coordinator or his bank account; 3) extension of duration of action; 4) any significant change of Annex 1 or Annex 2.

Change requests can be initiated by any partner and should begin with a written (e-mail) request to the project office. The formulation of the change request will first be negotiated by the project office with the partner in question. In addition, on a case by case basis the project coordinator will deem whether changes must be ratified by the EB and/or the GA.

Once the change request has been formulated to the satisfaction of all parties involved the formal change request will be submitted as governed by the Grant Agreement Article 39:

- 39.1 Conditions
  - The Agreement may be amended, unless the amendment entails changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.
  - Amendments may be requested by any of the parties.
- 39.2 Procedure
  - The party requesting an amendment must submit a request for amendment signed in the electronic exchange system.
  - The coordinator submits and receives requests for amendment on behalf of the beneficiaries.
  - The request for amendment must include:
    - The reason for the request
    - The appropriate supporting documents

4.4 Project Meetings

Project meetings are set periodically, as indicated in the DoW, or exceptionally, depending on the project needs, at different levels. Following types of project meetings are foreseen (other may be possible depending on project activities):

- General Assembly Meetings: All the partners involved in the Project are expected to take part in the periodic GA Meetings. Such meetings are chaired by the Project Coordinator and will involve at least one representative per partner. General Assembly meetings are generally planned every four months.
- WP(s) Meetings: Each WP leader calls for physical or virtual meetings of the WP once every month or whenever required for the coordination of the effort inside the WP. Meetings could be also organized at any time in the case of an emergency situation. The WP leader should give each of the members of the WP at least ten (10) calendar days' notice and provide in a timely fashion an agenda. WP leader is required to keep and report the WP meeting's minutes in the appropriate Wiki page.
- Review Meetings (including preparation days).

The templates for meeting agenda and minutes are available in the project workspace.

Meetings may also be held by teleconference or any other telecommunication means. Remote meetings, such as audio or web conferences, will be held periodically, depending on what established during the Plenary Project meetings.

Specific virtual meetings can be arranged depending on particular needs of the Project.

The invitation (containing information to connect to the meeting) as well as the agenda will be circulated not later than a couple of days before the meeting; the minutes will be prepared in the format of an e-mail and circulated immediately after the conference. No further (strict) constraint is established in order to avoid a bureaucratic overhead.

4.5 Project Workspace

The primary project workspace will be a Microsoft Teams (MS Teams) instance hosted through the project coordinator AIT. This workspace will provide document sharing and joint document authoring capabilities to the consortium.

There is a “General” workspace (referred to as a “channel” within MS Teams), managed by the project coordinator, providing read-access to all project-relevant materials to the consortium. This includes for example all document templates, project logos, and contractual documents.

There are also work package channels (WP1, WP2, WP3, WP4, WP5) that will be administered by the work package leaders. These channels will be used to store WP-related materials (e.g., meeting minutes) and manage and jointly author WP deliverables.

In addition, MS Teams will be the primary tool for video conferencing in the project.

5 Risk Management and Quality Assurance

5.1 Overview Risk Management

Anti-FinTer will perform continuous evaluation throughout the project, identifying any possible problems/risks at an early stage so that solutions can be elaborated in time. A systematic approach is to be adopted for monitoring resource spending against project budget and for achievements against schedule and critical success factors.

A Risk Management process will be defined with the following main elements:

- A **Risk Register** is set up to specify and identify risk management procedures and responsibilities;
- **Risk Identification**, that aims to identify risks of any nature that might occur in the project;
- **Risk Analysis**, that evaluates the likelihood and the severity of each risk and its potential impact on the project;
- **Mitigation Actions**, that aims to identify the measures and the processes should be undertaken to manage risks. Mitigation actions define who is responsible for the risk and the scope of the mitigation action;
- **Monitoring Results** is the process of keeping track of the risks and evaluating the effectiveness of the mitigation actions. Monitoring may also provide a basis for developing additional response actions and identifying new risks. This will also take place continuously, throughout the project.

The identified risks and mitigation measures will be reviewed in the regular EB and GA meetings. Detailed information about Risk Management will be provided in "D1.2 - Quality Assurance Plan" due in M3.

5.2 Overview Quality Assurance

Ensuring an affordable planning and good quality to the overall project results is part of the overall management mandate.

The main objectives of the Anti-FinTer quality assurance policy are:

- to implement and maintain a quality system
- to identify for all partners involved their responsibilities regarding quality
- to ensure that all deliverables comply with the grant agreement
- to ensure that all processes relevant to the project are organised and monitored to a high level of effectiveness and quality.

5.2.1 Document Templates

The following document templates have been created and made available to the consortium through the project workpace. These templates should be used by all partners where appropriate:

- Deliverable Template (MS Word)
- Deliverable Review Form Template (MS Word)
- Meeting Agenda Template (MS Word)
- Meeting Minutes Template (MS Word)
- Project Presentation Tempate (MS PowerPoint)

Detailed information about Anti-FinTer Quality Assurance will be documented in "D1.2 - Quality Assurance Plan" due in M3.

6 Conclusions

This Project Handbook details the Anti-FinTer project, the consortium, the project activities and KPIs, management and decision-making structures, project monitoring and reporting procedures. It provides consortium partners with a commonly shared operational methodology, and a set of management rules and guidelines to be adopted in order to manage and carry out the activities and fulfil the contractual obligation towards the European Commission, while at the same time reducing the overhead and increasing the efficiency and quality of the work carried out.

Additional project deliverables due in M3 will supplement and support this Handbook through a Quality Assurance Plan, providing guidelines on software development and document management, including deliverable management (D1.2), through Ethical Requirements and a Code of Conduct that will provide internal guidelines necessary to ensure that the consortium pays appropriate attention to the effects of the project on individual rights and freedoms (D1.3), and through the Dissemination, Communication and Outreach plan that will describes the communication methods, target groups, and messages (D5.1).