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

D1.2 Quality Assurance Plan

WP number and title	WP1 – Project Management
Deliverable number	D1.2
Version Number	1.0
Document Reference	Quality Assurance Plan
Lead Beneficiary	AIT
Deliverable type	R
Planned deliverable date	2022-03-31
Date of Issue	2022-03-31
Dissemination level	PU
Authors	AIT
Contributor(s)	IANUS
Keywords	Quality assurance, quality plan, risk management, risk assessment, project management

This project has received funding from the by the European Union's Internal Security Fund — Police under Grant Agreement No. 101036262

Consortium Partners

The Anti-FinTer Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Country
1	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

Document History

Version	Date	Status	Author(s), Reviewer	Description
V0.1	2022-02-24	Draft	Michela Vignoli	First draft
V0.2	2022-03-02	Draft	Ross King	Updated draft for review
V0.3	2022-03-17	Reviewed	Georgios Kioumourtzis	Review
V0.9	2022-03-23	Released	Michela Vignoli	Final version
V1.0	2022-03-21	Final	Ross King	Submitted version

Table of Contents

1 Introduction 6
1.1 Purpose of the Document 6
1.2 Scope and Intended Audience 6
1.3 Structure of the Document 6
1.4 Related Documents 6
2 Quality Management 7
2.1 Quality Plan for Internal communication 7
2.1.1 Communication tools 7
2.1.2 Prior notice of planned publications 8
2.2 Quality Plan for External Communication 8
2.2.1 Roles and responsibilities of project partners 8
2.2.2 Public Dissemination 8
2.2.3 Communication with specialists 9
2.2.4 Open Access Publishing 9
2.3 Quality Plan for Document Management 9
2.3.1 Document Standards 10
2.4 Deliverable Workflow 11
1.1.1 Deliverable Manager 12
1.1.2 Deliverable Reviewer 12
2.4.1 Deliverable quality and reviewer role 12
1.1.3 Deliverable Timing 12
3 Risk Management 14
3.1 Risk Identification 14
3.2 Risk Categorisation 14
3.3 Risk Assessment 14
3.4 Risk Mitigation 15
3.5 Risk Monitoring 15
3.6 Risk Register 16
3.7 Roles and Responsibilities 16
3.7.1 Risk Manager 16
3.7.2 Executive Board (EB) 17
3.7.3 General Assembly (GA) 17
3.7.4 Project Partners 17
4 Conclusions 18

List of Tables

Table 1: Deliverable Workflow 13
Table 2: Risk Probability and Impact Matrix for Unmitigated and Mitigated Risks 15

1 Introduction

1.1 Purpose of the Document

Deliverable D1.2 "Quality Assurance Plan" describes the quality management and risk management procedures applied in the Anti-FinTer project. This deliverable sets the guidelines for ensuring and evaluating the quality of work and deliverables, and for assessing internal and external risks related to the project. This document describes related responsibilities and actions that need to be fulfilled by all Anti-FinTer consortium members.

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. 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

In **Chapter 2 – Quality Management**, quality plans for internal and external communication are detailed, including adopted tools, roles, and responsibilities of project partners. Quality assurance also includes standards for project documents and details the required deliverable workflow.

Chapter 3 – Risk Management Plan provides a management framework to ensure that levels of risk and uncertainty are properly managed for the project. As risk management is an ongoing process over the life of a project, the Risk Register must be considered a 'snapshot' of relevant risks at one point in time.

1.4 Related Documents

Quality Assurance and Risk Management are integral parts of the overall project management process. The overall Project Management structure of Anti-FinTer is presented and detailed in D1.1 Project Management Handbook (M1).

The Dissemination, Communication and Outreach plan (D5.1, M3) describes the communication methods, target groups, and messages as well as the list of planned Dissemination activities. It complements the Quality Plan for External Communication provided in chapter 2.2.

Since the project has the potential to be highly controversial as it deals with the highly charged topic of terrorism, additional Dissemination Guidelines have been shared with the consortium.

It is important to note that any rules and regulations presented within this Project Risk Management and Quality Assurance are supplementary to the Consortium Agreement as well as the Grant Agreement. Many items regulated there are NOT repeated here but should be taken into account.

2 Quality Management

2.1 Quality Plan for Internal communication

The project requires clear and transparent communication between partners. Day-to-day communication and distribution of intermediate results will be carried out mainly by e-mail and file sharing via the project MS Teams site.

2.1.1 Communication tools

This section describes the main tools that are adopted in the project in order to assure an efficient internal communication. These are: MS Teams and SharePoint for conference calls and collaborative editing, and electronic mail.

2.1.1.1 MS Teams

Anti-FinTer adopted Microsoft Teams as a central web-based communication platform. The Anti-FinTer Teams is a cooperative working area, private and reserved to the project partners. Access is controlled by login and password, which are assigned by the site administrator (AIT).

MS Teams acts as the primary means of communication for the delivery and exchange of content/information. In many cases, deliverables could be prepared directly in Teams, respectively on the connected SharePoint instance hosted at AIT, and finally moved to a PDF format for their final delivery.

All project participants are granted access to the shared workspace. Each project partner is responsible to notify AIT of changes of project participants in his/her organization. Project partners are allowed to add additional contents/pages to the Redmine workspace where appropriate.

WP leads will be given full control over their own sub-project site. They may determine who has write access to this site and may construct it according to the WP needs.

The **central document repository on Teams** allows the Anti-FinTer partners to share, upload, download, and collaboratively edit documents concerning project activities. To the extent possible, project documents should be stored in this central library (and not in the sub-project areas).

Overview of main shared folders:

1. Consortium Agreement – this folder contains the Consortium Agreement
2. Deliverables – this folder contains the public deliverables of the project
3. Executive Board – this folder contains the agendas and minutes from the EB calls
4. Grant Agreement – this folder contains the Grant Agreement (and associated appendices, including the Description of Action)
5. Meetings – this folder contains the agendas, presentations, and minutes from all project meetings
6. Presentations – this folder contains a genera project presentation and other presentations relevant for the project
7. Publications – this folder contains publications to be submitted and to be reviewed by the consortium
8. Relevant Papers – this folder is used to share relevant papers within the consortium
9. Reporting – this folder contains the effort and activity reports from all partners
10. Templates – this folder contains the templates for the Anti-FinTer project documentation

It is a general principle that documents should be uploaded to the Documents area and then announced by email rather than attaching them to emails.

2.1.1.2 Electronic Mail

Mailing lists are a major means of communication within the project. They are preferred to listing the addresses.

- In order to prevent misuse of these email lists, all email lists are closed lists, i.e., only members (email addresses) registered for a particular list may send messages to the list.
- As a general policy each person posting to any of the email lists should ensure that the content of the message is appropriate for the recipients of the list selected, thus avoiding unintended and unnecessary emails.
- Emails sent to the email lists will be archived at an email server of AIT.
- All email lists will automatically add an appropriate prefix to the email header to ensure they can easily be identified as list emails of the specific list.
- For non-list communication, please put [Anti-FinTer] in the subject line.

Several email lists will be defined from the start. In addition to these lists further email lists may be established for other purposes needed. AIT will administer these lists and requests for mailing lists should be sent to the Project Manager.

2.1.2 Prior notice of planned publications

The Anti-FinTer consortium agreement states that prior notice of any planned publication shall be given to the other Parties at least 45 calendar days before a written publication and 21 calendar days before a presentation. The Teams folder “Publications” will be used for that purpose. The authors are requested to share the submitted version with the consortium in due time.

The submitted version should be added to the “Publications” folder, and a notification with a link to the publication should be sent to the anti-finter@list.ait.ac.at mailing list.

Any objection to the planned publication shall be made via e-mail to the Coordinator and to the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice of the written publication, and 15 calendar days in case of receipt of a notice of a presentation.

2.2 Quality Plan for External Communication

2.2.1 Roles and responsibilities of project partners

AIT is the official press contact of the project. As a general rule, partners should always consult all press releases and large-scale dissemination activities (including on the national level) with WP5 leader (IANUS) and the Coordinator (AIT). A standard communication text that can be used by all partners for general communication about the project will be provided. Any communication going beyond what is included in this general communication text must be delegated to the project coordinator.

As a general rule, LEA participation at events must not be announced before the event.

The dissemination guidelines defined for the project must be adhered to. These guidelines and additional details on external project communication and the project’s dissemination strategy are included in the Dissemination, Communication and Outreach plan (D5.1).

2.2.2 Public Dissemination

The aim of public dissemination of Anti-FinTer will be to inform about the project and its general developments. As the project focuses on a sensitive matter (terrorism), care must be taken when communicating with the public and media in order to avoid unnecessary misunderstandings about the nature of the project and incorrect perception of its activities. The partners must be aware, that the online

communities (as embodied for example on discussion forums, or comment threads on news websites) can easily misunderstand and misrepresent potentially controversial projects (and Anti-FinTer is one of them, as it involves virtual currency tracking, LEAs, as well as privacy and security issues).

In general, we should be restrictive as possible about how we are achieving impact. In this context it is important to consult the project stakeholders far in advance of publishing any information about project results (e.g., developed technologies, use cases derived from concrete prosecution cases).

2.2.3 Communication with specialists

The primary focus of Anti-FinTer's external communication will be to communicate with specialists in the field, who are already familiar with the problem and related issues (i.e., the scope for misunderstanding of the project will be limited, and the communications will be private and confidential). It will be much easier to maintain confidentiality and non-disclosure clauses in communicating with stakeholders as opposed to the media and the general public. Due to relatively low number of stakeholders, the communication with them will likely be personal and private (as opposed to the contacts with the media and public in communication and general dissemination activities). The stakeholders can be provided with a brief overview of the project, and when providing detailed project information, an NDA (non-disclosure agreement) can be signed between a stakeholder and the consortium. All direct emails should include a clause of confidentiality.

Stakeholders will be approached through the existing professional networks of the project partners. New stakeholders will be also met by the partners in various trade shows, conferences, and similar events.

2.2.4 Open Access Publishing

We encourage all project partners to ensure open access to peer-reviewed scientific publications relating to their results. Participants can choose between two routes:

- **Self-archiving** (also referred to as 'green' open access), meaning that a published article or the final peer-reviewed manuscript is archived (deposited) in an online repository before, alongside or after its publication. If this route is chosen, beneficiaries must ensure open access to the publication within a maximum of six months (twelve months for publications in the area of social sciences and humanities).
- **Open access publishing** (also referred to as 'gold' open access) means that an article is immediately placed in open access mode (on the publisher/journal website). Publishers often charge so called Article Processing Charges to make articles open. Such costs are eligible for reimbursement during the lifetime of the project as part of the overall project budget. For gold open access publishing, open access must be granted by the date of publication at the latest. A copy should, at the same time, be deposited in a repository.

2.3 Quality Plan for Document Management

The aim of this chapter is to describe the document management procedure for the Anti-FinTer Project. It defines standard rules and procedures related to document production that all the partners shall apply throughout the project.

The document management procedure is applicable:

- to all partners,
- for all deliverable documents to the European Commission,
- and for documents exchanged between partners.

It is recommended that documents internal to the consortium follow these guidelines as well. This chapter specifically deals with the procedures for release of project documents.

2.3.1 Document Standards

2.3.1.1 General

In order to improve efficiency, we suggest the use of standard tools. The following tools are recommended:

- Word processing: MS Word
- Spreadsheet: MS Excel
- Slide-based presentation: MS PowerPoint
- Document for web publication: PDF

2.3.1.2 Document Naming Conventions

The naming convention for deliverables is as follows:

Anti-FinTer_DX.Y

Where **DX.Y** is deliverable number according the DoA.

The naming convention for meeting minutes is as follows:

Anti-FinTer_type _date

Where

type is one of the following meeting types

- GA = General Assembly
- EB = Executive Board
- WPN = Work package, N = WP number

date is the date on which the meeting took place (ISO 8601)

For example, the code Anti-FinTer_GA _2022-02-21 indicates: minutes from the General Assembly meeting held on February 21, 2022.

The naming convention for general documents is as follows:

Anti-FinTer_type_partner_date

Where

type is the document type, for example

- ActivityReport
- EffortReport
- ShortPresentation
- Etc.

partner is the optional short name of the author organisation of the document

date is the date on which the document was authored. (ISO 8601)

For example, the code Anti-FinTer_ActivityReport_AIT_2022-09-03 indicates: the 6-month Activity Report of AIT, authored on September 3, 2022.

2.3.1.3 Document Presentation

Standard documentation templates will be used by all partners in order to produce standardised documentation. These templates are provided in the “Templates” folder on MS Teams.

All Anti-FinTer documents have standard format, including a document log. Each document will contain:

- a title page,
- a document status sheet and change record table (for evolutionary documents only),
- an (executive) summary,

- a list of applicable documents and reference documents (with version and date for technical documents),
- annexes if applicable.

The **ISO 8601** standard for dates will be used for all documents, e.g., **2017-06-10** for June 10, 2017.

When a document is issued for the first time, it should be defined as a draft (Version 0.x). Usually, the approval process requires that a document is circulated for comments among the interested partners. Upon receiving the comments by the specified deadline, the author will make the proper modifications, therefore changing the version sub-number, without the main number.

Normally, only the first official release of a document will be called V1.0, when this document will receive the final approval by the designated internal reviewer (so-called **Reviewer**).

Dissemination Level
This attribute reflects the level confidentiality as defined in the Grant Agreement:

- **CO**: Confidential; Internal circulation within project
- **PU**: Public document.

Document Status
The status of a document is determined by the document owner; in the case of a Deliverable this is the Deliverable Manager. The possible statuses of a document are:

- Draft
  - While being authored by the Deliverable Manager
  - Handed over to the Deliverable Reviewer in this state
- Reviewed
  - After review by the Deliverable Reviewer
  - Handed back to the Deliverable Manager in this state
- Released
  - After the Deliverable Manager has integrated and responded to the Reviewer comment
  - Handed over to the Project Coordinator in this state
- Final
  - Version submitted to the EC continuous reporting system by the Project Coordinator

The above status values appear on the document presentation page.

Internal Deliverable Status
After delivery the status of the document becomes:

- Delivered
- Accepted, Accepted with remarks, or Refused
- Final

The above status does not appear on the document but are managed internally.

2.3.1.4 PowerPoint Presentation

A template for presentations has been defined and it is available in the “Templates” folder on Teams. It should be used for presentations within the project as well as for external presentations (conferences, training, outreach, etc.) connected to the project.

2.4 Deliverable Workflow

Usually, the deliverables in a collaborative project are written with contributions from several partners. In order to minimize the effort for handling such documents, it is important for all participants to follow agreed-upon standards for formats and tools as well as procedures to be used in document editing and exchange.

1.1.1 Deliverable Manager

Each deliverable must have a **Deliverable Manager** who will coordinate the production of the document, interacting as necessary with the other partners involved. The Deliverable Manager will be documented on the Anti-FinTer Deliverable Development Plan on Teams.

1.1.2 Deliverable Reviewer

For each deliverable in a WP, the Deliverable Manager and the WP Leader suggest a person inside the project (but outside of the Work Package) as **Reviewer**. The Reviewer will also be documented on the Anti-FinTer Deliverable Development Plan on Teams.

2.4.1 Deliverable quality and reviewer role

During the production of the deliverable, there may be other intermediate phases where the Reviewer is asked to check partial drafts, but mainly because of time constraints this cannot be established as a rule. During the whole process of draft production, the Deliverable Manager will be the only person responsible for checking the technical quality of the deliverable as it progresses.

The Reviewer will check the Deliverable from the following points of view:

- The Deliverable covers the objectives stated in the DoA
- The Deliverable is complete (there are no missing parts, non-existing references, topics not covered, arguments not properly explained)
- The Deliverable addresses documented User Requirements
- The quality of the work described in the document is acceptable and is in accord with what was expected

A deliverable review form is provided in the “Templates” folder on Teams.

1.1.3 Deliverable Timing

The Deliverable Manager will define the document structure and the contributions expected from each contributing partner and will define a plan of the meetings and activities he/she may consider necessary for the development of the deliverable.

Upon receiving the input from the different contributors, the Deliverable Manager will merge them into a single document. Deliverables must use the standard template provided in Redmine. This first draft will then be circulated and asked for comments. Each partner will check its consistency with the plans and give their feedback and approval.

This iterative procedure will be repeated as necessary, until all involved partners have given their approval to the Deliverable Manager. The Deliverable Manager will then prepare a final draft (status “Validated”), which will then be sent for the internal review to the defined Reviewer, who may reiterate and re-circulate the deliverable as required until the necessary quality level is attained.

Then the final version of the deliverable (status “Released”) is sent to the Coordinator, who will submit a PDF version the Deliverable to the online submission system, thus making it available to the Project Officer (PO) and the project reviewers. The Deliverable will also be archived in Redmine and thus be made available to the consortium.

Deliverables must be provided to the Commission according to the delivery date specified in the Description of Work. After Deliverables have been officially accepted by the commission (that is, after a formal review), they achieve the status “Final.”

Action	Responsible	Deadline
Define Deliverable Manager	WP Lead	At least 3 months before external deadline
Define Reviewer	WP Lead & Deliverable Manager	At least 3 months before external deadline
Release final draft to Reviewer	Deliverable Manager	4 weeks before external deadline
Release final version to Coordinator	Reviewer	10 days before external deadline
Deliver Deliverable Submission Sheet to Project Officer; archive PDF version in Redmine	Coordinator	By external deadline
Make Deliverable available on the website if PU	WP7 Lead	After successful review by the Commission

Table 1: Deliverable Workflow

3 Risk Management

3.1 Risk Identification

Risk identification involves determining which risks or threats are likely to affect the project. It involves the identification of risks or threats that may lead to project outputs being delayed or reduced, outlays being advanced or increased and/or output quality (fitness for purpose) being reduced or compromised.

Multiple ways for accomplishing this step are available, ranging from engaging the project team in a brainstorming session, to consulting experienced team members, and to requesting opinions of experts not associated with the project. Typical methods of identifying risk are expert interviews, reviewing historical information from similar projects, conducting a risk brainstorming meeting, and using more formal techniques such as the “Delphi method”.

Risk identification in Anti-FinTer is realised with the engagement of experienced team members. Risk identification is discussed at Executive Board (EB) level, and involves key task leads from all WPs. Any partner can propose risks by contacting either their WP lead or the project Coordinator.

All identified risks are added to the running Risk Register on MS Teams that is continuously updated. Risks and their associated mitigation measures are evaluated and trends (an increase or decrease in the risk probability) are noted.

3.2 Risk Categorisation

Project planning outputs – scope, cost, time, and quality baselines – are what is at risk. Having full knowledge of them is crucial in developing response plans to counter risks to which the outputs will be exposed. These risks can be organized into different categories. In Anti-FinTer risks will be classified according to their effect on the project – scope, quality, and schedule.

3.3 Risk Assessment

Once risks have been identified, it is important to determine both the probability that each of the risks will occur, and the impact to the project if they occur. In order to determine the severity of the risks identified, a probability and impact factor has to be assigned to each risk. This process allows the project manager to prioritize risks based on the effect they may have on a project.

For our risk assessment, we use qualitative criteria in a nonnumeric probability scale (HIGH, MEDIUM, LOW). Probability is assessed for both unmitigated and mitigated risk scenarios (see Table 2). The unmitigated and mitigated probability and impact assessment for each risk is documented in the Risk Register.

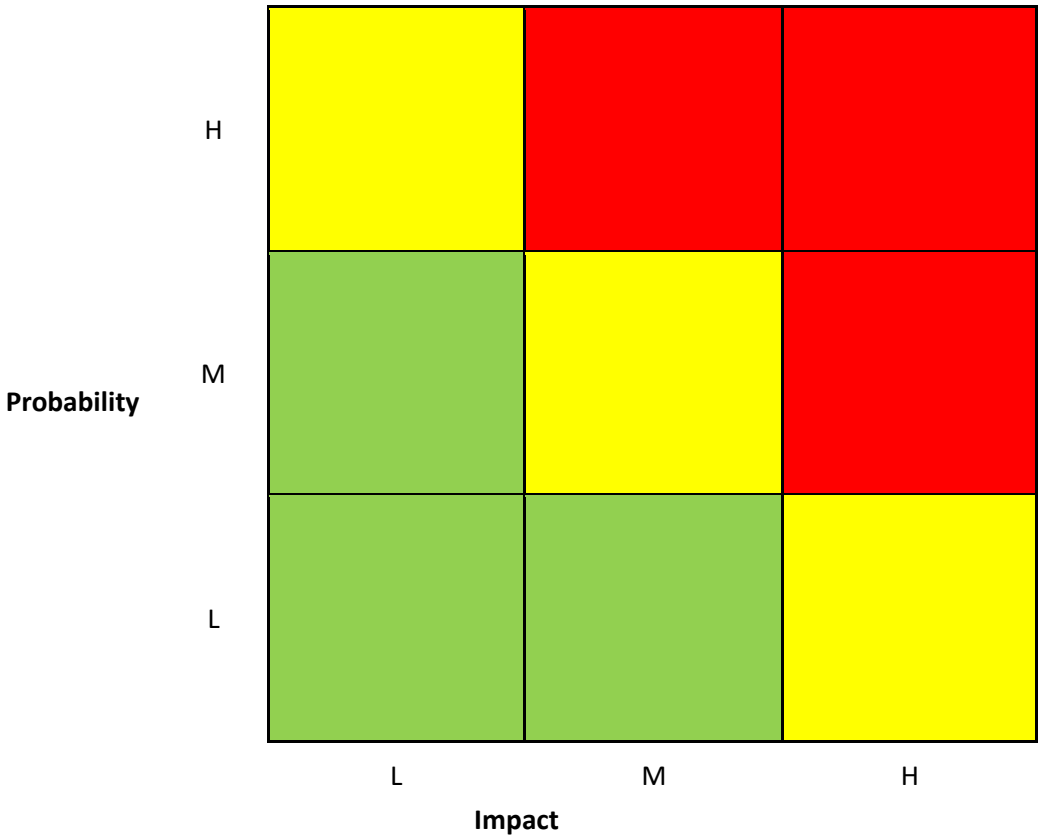

Table 2: Risk Probability and Impact Matrix for Unmitigated and Mitigated Risks

3.4 Risk Mitigation

Once risks have been qualitatively defined, the project team must determine how to address the risks that have the greatest potential for affecting the project. This section of the risk management plan explains the response options and actions that are available to the project team in managing the risks.

The intent of risk mitigation is to lower the probability or impact (or both) of an unfavourable risk event to an acceptable threshold. A fairly common risk for many projects is the potential decision delays caused by the busy schedules of the project.

This risk can be mitigated by a number of ways, such as reducing the number of major milestone decision points or the delegation of decision authority to one of the executive's direct reports.

A mitigation strategy is defined for each risk and documented in the Risk Register. Mitigation measures are discussed at EB level and at GA level.

3.5 Risk Monitoring

Most of a project managers attention with respect to risk management tends to focus on the activities associated with risk identification, risk assessment, and risk response planning. Where project managers historically spend less time and focus are the activities associated with risk monitoring. It is not uncommon, that project managers continue to be surprised when a risk event they had identified earlier, but were not monitoring, suddenly turns into an issue. To protect against this, diligent risk monitoring must be a part of every project manager's activities and he or she must have tools in their Project Management Toolbox to effectively perform this function.

There are four primary elements involved with risk monitoring activities: (1) systematically track the status of risks previously identified; (2) identify, document, and assess any new risks that emerge; (3) effectively

manage the risk reserve; and (4) capture lessons learned for future risk identification and assessment efforts. These monitoring activities are carried out in the regular EB calls, where risks are dynamically monitored and reassessed. Potentially emerging (new) risks are assessed so to ensure execution of the project according to the project plan with its Milestones and critical paths. In addition, the Risk Register is discussed at the regular GA meetings.

3.6 Risk Register

The Risk Register provides a record of identified risks relating to a project and serves as the central repository for all open and closed risk events. The Risk Register typically includes a description of each risk event, a risk event identifier, risk assessment outcome, a description of the planned response, and summary of actions taken and current status.

The Anti-FinTer Risk Register is provided in spreadsheet format. The main elements of the register are the following:

- **Risk Identifier**: Each risk will have a unique identifier for cataloguing and monitoring purposes.
- **Risk Description**: The risk description is related to the identification of risk events. We will use the "IF/THEN" format not only to describe the risk, but also to describe the potential consequences: "IF" this occurs (risk event), "THEN" that will be the outcome (consequences).
- Raised by
- **Dates**: For each risk the date that the risk was identified, and the date when the risk was last reviewed are documented.
- **Unmitigated Probability and Impact**: As part of the risk assessment, probability, and impact of the risk for the scenario without mitigation strategy in place is determined.
- **Risk Owners**: Every risk event, regardless of priority, will have an owner assigned. The risk register therefore will provide the owner component. The risk owners are the persons who are responsible for monitoring the risk event and initiating the risk response action if and when it is necessary.
- **Mitigation Strategy**: A mitigation strategy is defined for each raised risk and discussed at EB level.
- **Mitigated Probability and Impact**: As part of the risk assessment, probability, and impact of the risk with mitigation strategy in place is determined.

3.7 Roles and Responsibilities

3.7.1 Risk Manager

The Risk Manager (AIT) works closely with the WP leads for the early identification of project implementation risks and the mitigation measures to be applied.

The Project Risk Manager is be responsible for:

- Development and implementation of a Project Risk Management Plan
- Organisation of regular risk management sessions so that risks can be reviewed, and new risks identified
- Assessment of identified risks and developing strategies to manage those risks for each phase of the project, as they are identified
- Ensure that risks given high priority are closely monitored
- Providing regular Status Reports to the Project Coordination Group noting any risk with high severity and specifying any changes to the risks identified during each phase of the project and the strategies adopted to manage them

3.7.2 Executive Board (EB)

The EB reviews the project risks on a monthly basis via updated information provided in the EB meetings and provides advice and direction to the project Coordinator. The EB is provided with an updated Risk Register for consideration, as required, when additional threats emerge or the likelihood or potential impact of a previously identified risk changes.

3.7.3 General Assembly (GA)

The GA reviews the running Risk Register at the bi-annual GA meetings. If the risks cannot be solved at EB level, they will be escalated to GA level at any time in the project.

3.7.4 Project Partners

All members of the Project Team are responsible for assisting the Project Risk Manager in the risk management process. This includes the identification, analysis and evaluation of risks and continual monitoring throughout the project life cycle.

4 Conclusions

In this document, we presented the main components of the Anti-FinTer Quality Assurance and Risk Management plan.

We elaborated on the how quality management will be realised by providing goals and associated metrics along with quality control mechanisms.

We also provided guidance on document handling and quality control procedures along with specific responsibilities.

The production of project deliverables, the methodology to be followed by project partners with associated templates were also discussed in detail.

In the second part of this deliverable, we provided a management framework to ensure that levels of risk and uncertainty are properly managed for the project. An essential part of risk management is related to risk assessment, in which we discussed how a risk is assessed in terms of probability of occurring (likelihood), its impact, and related mitigation measures. The Anti-FinTer Risk Register is a rolling document available online in the project shared repository for easier access and review by all responsible functions and partners.