

FERMI

FAKE NEWS RISK MITIGATOR

Project acronym: FERMI
Project full title: Fake nEws Risk MIigator
Call identifier HORIZON-CL3-2021-FCT-01
Start date: 01/10/2022
End date: 30/09/2025
Grant agreement no: 101073980

D1.5 FERMI Project Management Playbook

Work package: 1

Version: 1.0

Deliverable type: R - Document, report

Official submission date: M2

Dissemination level: Public

Actual submission date: M2



Leading author(s):

Surname	First name	Beneficiary
Fikenscher	Sven-Eric	BPA
Stangl	Stephanie	BPA

Contributing partner(s):

Surname	First name	Beneficiary
Dimakopoulos	Nikos	ITML

Peer reviewers:

Surname	First name	Beneficiary
Evangelatos	Spyros	INTRA
Rauta	Jenita	PUCF
Argillander	Johanna	PUCF
Ames	Suvi-Tuuli	PUCF

Ethics reviewer:

Surname	First name	Beneficiary
Markopoulou	Dimitra	VUB

Security reviewer:

Surname	First name	Beneficiary/Affiliated Entity
Bouwknegt	Léonie	National Police of the NL

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
0.1	04/10/2022-07/11/2022	First Draft	BPA
0.2	14/11/2022	Peer Review	PUCF
0.3	07/11/2022-15/11/2022	Revised Draft	BPA
0.4	22/11/2022	Ethics Review	VUB
0.5	23/11/2022	Security Review	Léonie Bouwknegt
0.6	24/11/2022	Peer Review	INTRA
1.0	15/11/2022-30/11/2022	Incorporating Reviewer Feedback, Finalisation	BPA

Executive summary

This deliverable is called the “FERMI Project Management Playbook” (D1.5) and – in accordance with its title and the associated descriptions in the Grant Agreement – gives an overview of the project’s overarching cornerstones and to-be-coordinated proceedings. This includes the assignment of roles and responsibilities that are of special importance to key players within the consortium. More specifically, BPA has been selected as Project Coordinator, KU Leuven and VUB are FERMI’s Legal and Ethics Advisors (with KU Leuven mostly focusing on data protection and VUB mostly lending their expertise on ethics), INTRA serves as the project’s Quality Manager overseeing that all outputs – in writing and otherwise – are conceptualised and, if applicable, also submitted and disseminated in accordance with high standards and in due course, the role of Technical Manager has been assigned to ITML that will coordinate the technical and innovation proceedings and LC steps in as Dissemination Manager in charge of getting FERMI’s key messages across. The role of the Work Package Leaders is briefly discussed too.

Besides these key players within the consortium, the Project Management Playbook also lays out the duties of numerous committees and boards, including the Steering Committee (the key consultation body where all consortium members – under the stewardship of the Project Coordinator – will interact with one another to discuss the next steps and plan accordingly), the General Assembly, the Data and Knowledge Management Committee where the technical partners will coordinate under the leadership of the Technical Manager as well as the Security Advisory Board and the Ethics Advisory Board that will monitor all security and ethics proceedings.

It is clarified that the consortium’s internal communication will take place in the form of in-person meetings, online discussions (to-be-held on Microsoft Teams) and a content management system (OwnCloud) and is to be facilitated by a common visual identity.

Further project management building blocks that are described in this deliverable include the division of labour along the lines of the project’s Work Packages, deliverables and milestones (the latter two constitute key outputs that the above-mentioned partners and bodies, if necessary, will elaborate on, contribute to and monitor). As mentioned above, the project’s outputs are also subject to quality screening. This includes specific monitoring and reporting standards that aim at verifying the substance as well as the financial developments; a special focus will be on checking the quality of the project’s deliverables that address the consortium’s entire work.

If necessary, the outputs of the project, especially in the technical real, will also be overseen by the Technical Manager along the lines of a gradual innovation management process that identifies (mapping), analyses (scouting), assesses and exploits such outcomes (in full compliance with intellectual property rights).

Eventually, the risks the FERMI project is facing are briefly described, which, at this point, however, have not changed since the conception and finalisation of the Grant Agreement. Having said that, the Steering Committee will constantly re-evaluate the risks to ensure all partner are up-to-date on those and mitigation measures can be embarked on sooner rather than later.

Table of Contents

Executive summary	3
Table of Contents	4
List of tables and list of figures	5
Abbreviations	6
1 Introduction	8
2 Project Management.....	9
2.1 Project Management Structure and Responsibilities.....	9
2.1.1 Project Coordinator (PC)	9
2.1.2 Legal and Ethics Advisors	11
2.1.3 Quality Manager	12
2.1.4 Technical Manager	12
2.1.5 Dissemination Manager	13
2.1.6 Steering Committee (SC).....	14
2.1.7 General Assembly (GeA).....	15
2.1.8 Work Package Leads (WPLs).....	15
2.1.9 Data and Knowledge Management Committee (DKMC)	15
2.1.10 Security Advisory Board (SAB).....	17
2.1.11 Ethics Advisory Board (EAB)	24
2.2 Work Package Management	28
2.3 Project deliverables.....	28
2.4 Project Milestones.....	30
3 Project Communication.....	31
3.1 Project Meetings	31
3.2 Content Management System (CMS)	31
3.3 Communication tools	33
3.4 Visual identity	33
4 Monitoring, Reporting and Quality Assurance	35
4.1 Deliverable submission process	35
4.2 Internal Progress Reports	36
4.3 Periodic Reporting	36
5 Risk Management.....	38
6 Innovation	41
6.1 Technical and Innovation strategy plan	41
6.1.1 Technical management approach.....	41
6.1.2 Innovation management approach.....	41
6.1.3 Monitoring and coordination	43
6.1.4 General plan and tool description	44
6.2 Intellectual Property Rights (IPR) Management.....	48
6.2.1 (Joint) Ownership	49
6.2.2 Transfer of results	50
6.2.3 Access rights.....	50
6.2.4 Dissemination and Reporting.....	51
7 Conclusion.....	52
Annex A Fermi Deliverable Tracker.....	54
Annex B Review Template	58

List of tables and list of figures

Table 1: FERMI partners	9
Table 2: Sensitive information with security recommendation	17
Table 3: List of further sensitive deliverables	18
Table 4: List of SAB experts	21
Table 5: List of EAB experts	25
Table 6: WP overview	28
Table 7: List of project deliverables	29
Table 8: Project milestones	30
Table 9: Indicative timetable of physical project meetings	31
Table 10: Indicative project implementation risks and mitigation measures	38
Table 11: Open Innovation activities.....	43
Figure 1: Content Management System - Login page	32
Figure 2: First level structure.....	33
Figure 3: Fermi logo.....	34
Figure 4: Deliverable submission process and timeline	36
Figure 5: Open Innovation Model	42
Figure 6: Innovation time-plan.....	45

Abbreviations

AB:	Advisory Board
AI:	Artificial Intelligence
BPA:	Bavarian Police Academy
BSP:	Bavarian State Police
CA:	Consortium Agreement
CDSL:	Cyber Data Security Lab
CFS:	Certificate on the Financial Statement
CiTIP:	Center for IT & IP Law
CMS:	Content Management System
EAB:	Ethics Advisory Board
EU:	European Union
DHPol:	Deutsche Hochschule der Polizei
DKMC:	Data and Knowledge Management Committee
GA:	Grant Agreement
GeA:	General Assembly
GDPR:	General Data protection Regulation
ICT:	Information and Communication Technologies
IPR:	Intellectual Property Rights
LEA:	Law Enforcement Agency
LLB:	Bachelor of Laws
LLM:	Master of Laws/Legum Magister
KIR:	Key Innovation Result
KER:	Key Exploitable Result
KPI:	Key Performance Indicator
LSTS:	Law Science Technology & Society
M:	Month
MRL:	Market Readiness Level
NLP:	Natural Language Processing
NTUA:	National Technical University of Athens
PC:	Project Coordinator
PCC:	Project Coordination Committee
PDM:	Project Dissemination Manager
PMP:	Project Management Professional
PSI:	Programme Security Instruction concerning Horizon Europe Programme
PSO:	Project Security Officer

QA:	Quality Assurance
RACI:	responsible, accountable, consulted, and informed
REA:	European Research Executive Agency
R-W-W:	Real-Win-Worth It
SAB:	Security Advisory Board
SC:	Steering Committee
SGM:	Stage Gate Model
SME:	Small and Medium Enterprises
T:	Task
TL:	Task Lead
TRL:	Technical Readiness Level
WP:	Work package
WPL:	Work Package Leader

1 Introduction

D1.5, the “FERMI Project Management Playbook” is expected to lay the ground for the project in the sense of describing the key coordination efforts that are aimed at streamlining the project and ensuring that its objectives are met. In the Grant Agreement’s description of the deliverable it is being argued that D1.5 should address quality, risk and innovation management. Accordingly, all of these dimensions are being described later on.

The quality management entails assurance mechanisms as to how to review the outputs of the project, especially the deliverables, which will be screened by two project reviewers in great depth (with experts on the security and the ethics side checking full compliance with the relevant norms and rules in both domains).

Innovation management (with a technical focus) is being carried out in view of an Open Innovation approach that requires the identification (mapping), analysis (scouting), assessment and exploitation of relevant project developments with sufficient innovation capabilities. Obviously, such efforts need to take place in strict accordance with the existing intellectual property rights, which are also addressed in this context.

Considering that the project risks have not changed since the conception and finalisation of the Grant Agreement (GA), such risks are described in line with the GA. Having said that, constant monitoring will ensure the early detection of new developments in the risk realm, which can pave the way for taking proper mitigation measures quickly enough.

Prior to all of these elaborations, however, the organisational structure of the project is laid out. This is the centrepiece of Work Package (WP) 1 which the FERMI Project Management Playbook is a part of. In this respect, the partners to whom roles and responsibilities of special importance have been assigned are being mentioned. This includes the Project Coordinator (BPA), the Legal and Ethics Advisors (KU Leuven and VUB), the Quality Manager (INTRA), the Technical Manager (ITML), the Dissemination Manager (LC) and the Work Package Leaders (WPL). These partners’ exact roles and responsibilities are laid out too.

The consortium’s work will be further discussed and coordinated within the framework of a set of bodies and committees with special obligations. Besides the overarching Steering Committee (SC, the project’s main consultation body) and the General Assembly (GeA, the project’s main decision-making body), in which all partners are involved, additional discussion and coordination groups are the technically-focused Data and Knowledge Management Committee (DKMC), the Security Advisory Board (SAB) and the Ethics Advisory Board (EAB).

The organisational structure also concerns internal communication proceedings (online and offline gatherings, a common repository, and the use of a common visual identity) and the assignment of partners to different Work Packages, deliverables and milestones in accordance with their expertise and duties as described in the Grant Agreement.

2 Project Management

2.1 Project Management Structure and Responsibilities

FERMI is a 36 month-long project, including 17 partners from 11 countries from the European Union (EU). The project brings together LEAs, academics, industries, research and technology as well as non-profit organisations.

Table 1: FERMI partners

No.	Participant organisation name	Short name	Type	Country
1	Hochschule für den öffentlichen Dienst in Bayern	BPA	RTO	DE
2	Atos IT Solutions and Services Iberia Sl	ATOS	INDUSTRY	ES
3	Netcompany-Intrasoft SA	INTRA	INDUSTRY	LU
4	Information Technology for Market Leadership	ITML	SME	EL
5	Inov Instituto de Engenharia de Sistemas e Computadores Inovacao	INOV	RTO	PT
6	Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH	BIGS	RTO	DE
7	Universita Cattolica Del Sacro Cuore	UCSC	ACADEMIC	IT
8	Ianus Consulting Ltd	IANUS	SME	CY
9	The Lisbon Council for Economic Competitiveness asbl	LC	NON-PROFIT	BE
10	Convergence	CONV	NON-PROFIT	EL
11	Vrije Universiteit Brussel	VUB	ACADEMIC	BE
12	Katholieke Universiteit Leuven	KUL	ACADEMIC	BE
13	The Police University College of Finland	PUCF	RTO	FI
14	Finland Ministry of the Interior	FMI	LEA	FI
15	Belgian Federated Police	BFP	LEA	BE
16	French Ministry of Interior	DMIA	LEA	FR
17	Swedish Police	SPA	LEA	SW

2.1.1 Project Coordinator (PC)

The role of Project Coordinator (PC) has been assigned to the Hochschule für den öffentlichen Dienst in Bayern (Bavarian Police Academy, BPA). The responsibilities of the PC (who also has to meet a set of obligations as a member of the consortium) are clearly laid out in the GA. More specifically, it is – among other things – explicitly stipulated that “[t]he coordinator must:

- (i) monitor that the action is implemented properly [...]
- (ii) act as the intermediary for all communications between the consortium and the granting authority, unless the Agreement or granting authority specifies otherwise, and in particular:
 - submit the pre-financing guarantees to the granting authority (if any)
 - request and review any documents or information required and verify their quality and completeness before passing them on to the granting authority
 - submit the deliverables and reports to the granting authority

- inform the granting authority about the payments made to the other beneficiaries (report on the distribution of payments; if required [...])

(iii) distribute the payments received from the granting authority to the other beneficiaries without unjustified delay [...].”¹

Against this backdrop, a key task of the PC is to communicate with the assigned Project Officer and EU institutions on behalf of the consortium. All consortium members are strongly encouraged to express any concerns within the framework of the project’s regular consultation and coordination efforts (including the specific bodies and committees as described below to ensure proper communication and the monitoring of specific obligations). Upon within-consortium consultation, however, it will be BPA’s job to share key developments and requests with the granting authority.

Besides the financial coordination, some of the further requirements the PC needs to meet when interacting with the granting authority (“submit the deliverables and reports to the granting authority” and “request and review any documents or information required and verify their quality and completeness before passing them on to the granting authority”) are seemingly linked to another core obligation of the PC, namely to monitor the project activities. It is clearly prescribed that these need to be “implemented properly”, which apparently alludes to the compliance with the Grant Agreement’s requirements as laid out in the description of the action,² in other words, the description of the different Work Packages, tasks, deliverables, overarching project objectives and Key Performance Indicators.

Accordingly, the PC has created – in close collaboration with the Quality Manager (INTRA) – a demanding review process that all key outputs in the form of deliverables need to go through before getting submitted. Considering that the wording above places a special emphasis on the role of the PC, it should be clarified here that BPA (along with INTRA) will receive all deliverables 15 days prior to the submission date from the lead beneficiaries so the result can be thoroughly reviewed. BPA staff will also be kept in the loop with respect to the preceding steps of the review process (in the sense of being cc’ed into the relevant email exchanges) and review some deliverables (in the capacity as a project reviewer) in greater depth even prior to their preliminary submission to the PC and Quality Manager. The specifics of the review process are described below (see chapter 4).

Besides the PC’s role in the deliverable review process, the PC will closely monitor the beneficiaries’ contribution to the to-be-submitted Technical Reports and the financial documents that the EC will receive.

To ensure that the PC is fully informed about all issues that may arise and that may need to be communicated to the granting authority in due course, BPA will regularly communicate with the consortium by email, in the form of telcos (that will be scheduled and moderated by BPA themselves if they concern all partners (see the remarks on the Steering Committee and the General Assembly below) and in which BPA will participate if they concern certain sub-dimensions of the project and will be scheduled and moderated by the partners in charge of those (as described below) and in-person meetings.

¹ Grant Agreement, General, p.25.

² The latter is presented in ANNEX 1, which is mentioned in Article 11 to which the remark above on the coordinator’s need to “monitor that the action is implemented properly (see Article 11)” alludes. More specifically, Article 11 states that “[t]he beneficiaries must implement the action as described in Annex 1 [emphasis added] and in compliance with the provisions of the Agreement, the call conditions and all legal obligations under applicable EU, international and national law,” see Grant Agreement, General, p.25.

2.1.2 Legal and Ethics Advisors

FERMI has two partners that advise the consortium on ethics and data protection issues, VUB and KU Leuven. The GA mentions that in the “[e]thics realm both partners act as “Legal Advisor(s).” Against this backdrop, they will be “monitoring the compliance of [the] project’s activities in respect to ethics, legal, privacy and data protection norms (including GDPR).”³ However, a distinction is made between the focal points of both partners’ involvement and expertise (although VUB and KU Leuven will clearly supplement each other’s work).

Interestingly, VUB will mostly focus on the ethics side, whereas KU Leuven will largely work on data protection issues. For example, VUB is introduced as the partner that will “complement the multidisciplinary consortium with their expertise on ethics as it derives from their Cyber and Data Security Lab (CDSL) and will be monitoring the research ethics throughout the project.”⁴ KU Leuven, on the other hand, is characterised as the partner that will be “providing [the] FERMI consortium with legal and ethical expertise to implement data protection requirements-by design at all stages of the project as well as conducting research and reflections on a fair balance of interest between law enforcement objectives and the protection of fundamental rights and democratic values, thus they are involved in tasks related to legal compliance, data management and contribute to setting FERMI’s baseline.”⁵

Accordingly, KU Leuven has the lead on T1.4 on “Data management and legal compliance”, whereas VUB has been entrusted with leading T1.5 on the “Continuous monitoring of research ethics.”⁶ The former obliges task leader and contributors (VUB and BPA) to identify “legal requirements which will need to be implemented within the project as well as constructing a data management plan for the research lifecycle of FERMI.” The Grant Agreement also requires that “KUL, as legal and ethical partner, will start by providing recommendations to ensure that end-user and stakeholder engagements, testing procedures, and piloting activities are legally compliant with the EU legal framework.” Eventually, this effort “will finalise information related to the types of data the project will generate and collect (including personal data), the standards that will be used to gather, transport and secure the data during the project, and determine how partners might exploit data post project-lifecycle (if appropriate).”⁷

T1.5, however, requires the task leader and the contributors (KU Leuven and BPA) to conceptualise “the ethics compliance protocol for the research lifecycle of FERMI.” More specifically, “[t]his task will result in an internal protocol for ethical procedures [...] to ensure adequate ethical standards are met through the research process. All partners will review the protocol and sign a letter of intent to adhere to the protocol. This task will organise the internal monitoring of the implementation of the ethics protocol by the consortium. The evaluation of this monitoring exercise will be reported during the projects’ interim and final reports.”⁸

KU Leuven and VUB – with the support of BPA that contributes to both tasks and all other partners, if required – will divide the labour in accordance with the descriptions above. One of the upcoming WP1 deliverables – D1.4 (“FERMI Data Management Plan”) – will contain the key results of both activities, namely the data management plan as well as the ethics protocol. Considering that VUB is leading the effort to oversee the project’s ethics proceedings and the compliance with these, it has been decided that VUB will chair the EAB where such monitoring activities will be coordinated, as described below.

³ Grant Agreement, Description of the Action, PART B, p.20.

⁴ Grant Agreement, Description of the Action, PART B, p.47.

⁵ Grant Agreement, Description of the Action, PART B, p.46.

⁶ Grant Agreement, Description of the Action, PART A, p.7.

⁷ Grant Agreement, Description of the Action, PART A, p.7.

⁸ Grant Agreement, Description of the Action, PART A, p.7.

2.1.3 Quality Manager

The Grant Agreement stipulates that a Quality Manager “will oversee conducting continuous quality assurance activities for the operation of the project and the production of its scientific and technical results within its lifespan.” First and foremost, “[t]his involves [...] developing, implementing, communicating, and maintaining the quality plan throughout the lifecycle of the project task.”⁹ Elsewhere in the Grant Agreement, in T1.3, to be exact, a partner is already appointed to that position. The task description prescribes that quality “procedures will be issued to be followed by the Quality Manager (INTRA)” that has also the lead on T1.3 (“Quality Control, Risk Management and Contingency Planning”).

The task description corroborates that INTRA, alongside the task contributors, will “monitor the work carried out during the project’s lifespan and guarantee compliance with high quality standards.” More specifically, some details as to how to conceptualise the above-mentioned quality plan are presented. The task description declares that quality standards “will refer to the: (i) control actions planned; (ii) time schedules; (iii) requirement specifications and quality objectives [that] will be clearly defined and documented; (iv) responsibilities and authorities [that] will be clearly defined; (v) development, quality, testing, configuration, acceptance and maintenance plans [that] will be defined and controlled; (vi) agreed definitions of procedures for acceptance and quality control [that] will be established; and (vii) appropriate tools for planning, monitoring and progress reporting [that] will be proposed.”¹⁰

In full accordance with the inner-consortium review process mentioned above, a special focus will be on organising proceedings that guarantee that all deliverables are submitted in high quality. To achieve this crucial objective “all the other partners will have to enrol in a peer review”.¹¹

Considering that the description of the FERMI Project Management Playbook requires the lead beneficiary and the contributors – in this case INTRA that agreed in coordination with the lead beneficiary BPA to take over this task – to lay out FERMI’s “QA [Quality Assurance] plan”¹² in detail, an overview thereof is provided later in chapter 4. This section remains limited to describing the essential roles and obligations within the consortium.

2.1.4 Technical Manager

Besides the management of ethics and quality issues, the GA also appoints a Technical Manager, namely ITML. This is clarified in T1.2, which states that the technical management “will be led by ITML, as the appointed Technical Manager.” This is a more than reasonable choice, given ITML’s achievements as a company “that provides novel, tailor-made software solutions based on a variety of technologies, such as Big Data Analytics, Advanced Data Mining technologies and Machine Learning, in numerous market fields.”¹³ In their capacity as Technical Manager ITML will not only oversee the project’s technical management, they will also form a project committee to coordinate on technical issues, the Data and Knowledge Management Committee, which “will support the innovation driven research and amplify the project’s impact.”¹⁴

⁹ Grant Agreement, Description of the Action, PART B, p.20. – Other dimensions of the Quality Manager’s work that are mentioned in the same context rather seem to concern the work of other managers or committees such as data management (which is overseen by KU Leuven) and curation and storage/preservation costs (which seem to fall into the circle of competence of the technical and financial management of the project).

¹⁰ Grant Agreement, Description of the Action, PART A, p.6.

¹¹ Grant Agreement, Description of the Action, PART A, p.6.

¹² Grant Agreement, Description of the Action, PART A, p.20.

¹³ Grant Agreement, Description of the Action, PART B, p.47.

¹⁴ Grant Agreement, Description of the Action, PART A, p.20.

Moreover, ITML will lead the above-mentioned task T1.2 on “Technical & Innovation strategic steering”, which entrusts ITML as well as the task contributors with presenting a “definition of the overall strategy of the project to achieve the technical objectives and the control of project progress with respect to those objectives. The overall strategy methodology will be broken down to specific strategies at a WP level to be settled with the respective WP leaders. According to new developments and ideas in the research areas considered by the project, the strategies are subject to adjustments and updates.”

More specifically, “[t]his task will produce a roadmap to be used as guidelines by the respective WPs to carry out their work [...]. ITML will lead the task by: (i) driving the technical activity, coordinating technical discussion among partners, ensuring consistency and complementarity of technical development, and settling technical conflicts; (ii) supporting the PC in reporting within all technical issues; (iii) arranging technical discussions and meetings with WPL; (iv) identifying technical risks and conflicts and taking of corrective actions supporting the PC in risk management activities. This task will also introduce and distribute guidelines for intellectual property creation, to ensure a consistent and transparent publication process of FERMI results towards innovation management.”¹⁵

Considering that the description of the FERMI Project Management Playbook requires the lead beneficiary and the contributors – in this case ITML that agreed in coordination with the lead beneficiary BPA to take over this task – to lay out FERMI’s “innovation plans”¹⁶ in detail, an overview of such plans can be found in chapter 6. This section remains limited to describing the essential roles and obligations within the consortium.

2.1.5 Dissemination Manager

The dissemination of project results is a priority for FERMI. The Dissemination Manager of the project is LC. According to the Grant Agreement, the “Dissemination Manager (LC) [...] [will be] responsible for all dissemination and communication actions of FERMI, including contact with stakeholders and synergies with other projects and initiatives.”¹⁷ The Dissemination Manager’s exact role and responsibilities are further specified in the description of T6.1. Among other things, T6.1 states that under the stewardship of the Dissemination Manager a “dissemination and communication roadmap of the project is designed to ease the coordination and management of the planned activities. The plan will include a variety of activities (e.g., participation in conferences, publications in journals, release of [a] newsletter, active presence of FERMI in electronic and social media, targeted contacts, and presentations to potential customers).”¹⁸

The GA mentions a whole series of further communication and dissemination-related focal points and also several exploitation measures that all translate into a set of highly ambitious Key Performance Indicators. It would be beyond the scope of this Project Management Playbook to address all of these items. From a coordination and management standpoint, it should suffice to emphasise the overarching output, which is a “a more detailed dissemination and communication plan”¹⁹ [that] will be established within the first six months of the project and will be updated annually.”²⁰

¹⁵ Grant Agreement, Description of the Action, PART A, p.6.

¹⁶ Grant Agreement, Description of the Action, PART A, p.20.

¹⁷ Grant Agreement, Description of the Action, PART B, p.46.

¹⁸ Grant Agreement, Description of the Action, PART A, p.13.

¹⁹ Just to clarify: The more detailed plan will build on the above-mentioned (initial) roadmap.

²⁰ Grant Agreement, Description of the Action, PART A, p.13.

2.1.6 Steering Committee (SC)

In the description of T1.1 the Grant Agreement requires the consortium to create an SC. As the GA further explains “[e]ach partner has a representative within the FERMI SC, which oversees the management activities.”²¹ In other words, the SC is going to be the main consultative body of the project, which includes all partners so they can coordinate their activities.

The Grant Agreement further clarifies some of the specific tasks the SC is meant to address. This list includes the following set of items:

- “taking care of the initial planning,
- monitoring the project for all its duration;
- monitoring deadlines and milestones;
- developing internal monitoring and report forms;
- fostering and guaranteeing information exchange and communication among partners;
- updating of the EU project website with information;
- taking care of the financial management.”²²

Some of these duties are self-evident and somewhat abstract focal points of a consultative body’s work such as “taking care of the initial planning,” “monitoring the project for all its duration,” “monitoring deadlines and milestones,” “fostering and guaranteeing information exchange and communication among partners,” albeit the requirement to keep an eye on deadlines and milestones makes a first attempt at specifying what proceedings the SC should pay particularly close attention to.

Having said that, ensuring that all deadlines and milestones are met and even more so the requirement to monitor the project as such “for all its duration” are obligations that hugely overlap with the PC’s above-mentioned commitment to “monitor that the action is implemented properly”, which, again, has been mostly addressed by initiating a thorough review process together with the Quality Manager (INTRA). The other rather general tasks of the SC also concern the role of the PC in the sense that planning and communication among consortium members is a clear prerequisite to ensuring that the project activities can be carried out in accordance with the Grant Agreement and that the granting authority can be informed in due course over any issues that may arise, as laid out above.

The nexus between the duties of the SC and the PC is at least as clear when it comes to the emphasis the GA places on “developing internal monitoring and report forms” and “taking care of the financial management.” Obviously, those two requirements are intertwined as far as the conception of internal monitoring and report forms that address financial matters is concerned. Just like any further (non-financial) internal monitoring and report forms these should help the PC meet one of the duties the Grant Agreement assigns to them, namely to “request and review any documents or information required and verify their quality and completeness before passing them on to the granting authority” (see the remarks on the role of the PC above). Monitoring and report forms that are to be used to evaluate the state of the consortium’s work and the outcomes thereof (that fall into the quality management process, see chapter 4) further advance the PC’s effort to ensure that all project requirements can be met in accordance with the GA.

These similarities notwithstanding, the PC is less concerned by another requirement that is laid out by stating the need to update “the EU project website with information.” This obligation will be fully addressed in the context of one of the project’s WPs that runs throughout FERMI’s entire duration, namely the one on

²¹ Grant Agreement, Description of the Action, PART A, p.6.

²² Grant Agreement, Description of the Action, PART A, p.6.

“[o]utreach management, exploitation and maximization of digital trust” (WP6).²³ Against this backdrop, there will be regular updates on the project’s communication and dissemination activities in the framework of the SC but the exact communication and dissemination process will be overseen by the Dissemination Manager (see section 2.1.5).

In view of the huge overlap between the PC’s duties and the SC’s tasks, the PC will oversee the work of the SC by scheduling, organising and moderating regular online (in the form of monthly telcos) and in-person meetings (envisaged to take place biannually, if circumstances allow). To sum up and conclude, the SC can function as the project’s main coordination forum, where all relevant proceedings are being elaborated on and the PC can inform consortium members about the exchanges with the granting authority as well as pressing requirements that need to be addressed. To ensure all partners are fully aware of the outcome of these discussions the PC will draft and share meeting summaries (capturing key takeaways and Action Points) with all partners.

2.1.7 General Assembly (GeA)

The General Assembly is the decision-making body of the consortium to which each partner assigns one representative (substitutes can be nominated, if necessary) that shall be deemed to be duly authorised to deliberate, negotiate and decide on all relevant matters. More specifically, the General Assembly will make decisions on topics such as content, finances, intellectual property rights, proposals for changes to Annexes 1 and 2 of the Grant Agreement to be agreed by the Granting Authority, changes to the consortium plan, additions, modifications or withdrawal of Background, additions to the list of Third Parties for simplified transfer and additions to the identified entities under the same control.²⁴

The PC will schedule the meetings of the General Assembly and draft the agendas (which, however, can be amended by the partners) and chair the sessions (unless the General Assembly makes a different decision). The General Assembly will meet regularly on a biannual basis but can also make decisions without a meeting. All meetings will be announced in due course and properly documented.²⁵

2.1.8 Work Package Leads (WPLs)

WPLs will manage and monitor the progress of the tasks of their WP through a continuous intermediation with the Task Leaders (TLs). They are responsible for the detailed planning of the subtasks and activities identified in the Grant Agreement and coordinate the to-be-conducted work. If necessary, the WPLs will schedule telcos with the TLs and further WP contributors to ensure sufficient communication and coordination between all partners whose work is of relevance to the WP as well as the proper organisation of all project activities. The WP management will be coordinated with the PC who will join WP-specific telcos whenever possible, which should further streamline the flow of information amongst the consortium members.

2.1.9 Data and Knowledge Management Committee (DKMC)

The DKMC also plays a very prominent role in the project. It is explicitly mentioned in T1.1. as one of the essential “project management bodies.”²⁶ Interestingly, other than the DKMC only the SC is alluded to in this context, which further speaks to the DKMC’s importance. With respect to the focal points of the DKMC’s

²³ Grant Agreement, Description of the Action, PART A, p.13.

²⁴ Consortium Agreement, p.13.

²⁵ Consortium Agreement, p.10-14.

²⁶ Grant Agreement, Description of the Action, PART A, p.6.

work it is being mentioned in T1.2 that the body “will support the innovation driven research and amplify the project’s impact.”²⁷ In other words, the key task of the DKMC will be to coordinate FERMI’s technical proceedings. Admittedly, the term “innovation” can have a rather broad meaning, which may exceed the boundaries of technical developments and cover cutting-edge social science research too.

However, the DKMC’s further description implies a clear technical focus. This is well-illustrated by assigning the role of chair to “the appointed Technical Manager,” namely ITML, that will be “leading [the] DKMC.”²⁸ Moreover, the Grant Agreement clarifies that the key responsibilities of the Technical Manager will include “coordinating [the] technical discussion among partners, ensuring consistency and complementarity of technical development, and settling technical conflicts.”²⁹ All of these tasks require in-depth coordination with the technical partners.

Having ITML chair a technically-focused DKMC appears to require that all partners that do critical technical work in the project are involved in the committee. This includes most of FERMI’s “Large Enterprises and [Small and medium Enterprises] SMEs Leading European Research and Development.”³⁰ Besides ITML the technically-relevant partners that fall into this category are

- INTRA as “one of the biggest IT service providers in Europe with a vast expertise in complex integration of software systems” that “brings their long experience in integrating complicated IT systems and their know how in Deep Learning and [Natural Language Processing] NLP”³¹ to the table and leads, among other things, the development of the FERMI Disinformation Sources & Spread Analysis and Impact Assessment modules as well as
- ATOS, which is a “well-known IT company from Spain providing innovative AI technologies” and, amongst other things, happens to be in charge of the FERMI Swarm Learning mechanisms.³²

Other partners with clear and crucial technical duties include

- INOV as “one of the largest national technological infrastructures in the field of Information and Communication Technologies (ICT) and Electronics [...] [with] their expertise on Safety and Security [...]. [INOV are intimately involved] in the technical tasks of the project such as developing the management model for community resilience to be integrated in the platform,”³³
- BIGS, which “offers, relevant experience in the application of methods to better measure the costs of extremism and the resulting benefits of various countermeasures involving civil society. Furthermore, BIGS [...] [will] lead the FERMI Behaviour Profiler & Socioeconomic Analyser,”³⁴ and
- UCSC, “more specifically the TRANSCRIME a joint research centre on transnational crime of the Università Cattolica del Sacro Cuore, the Alma Mater Studiorum Università di Bologna and the Università degli Studi di Perugia. They bring added value to the FERMI consortium with their expertise to lead WP3 and by utilizing their technological assets crime and more specifically in this case the [...] dynamic flows modeling of Disinformation.”³⁵

²⁷ Grant Agreement, Description of the Action, PART A, p.6.

²⁸ Grant Agreement, Description of the Action, PART A, p.6.

²⁹ Grant Agreement, Description of the Action, PART A, p.6.

³⁰ Grant Agreement, Description of the Action, PART B, p.47.

³¹ Grant Agreement, Description of the Action, PART B, p.47.

³² Grant Agreement, Description of the Action, PART B, p.47.

³³ Grant Agreement, Description of the Action, PART B, p.46-47.

³⁴ Grant Agreement, Description of the Action, PART B, p.47.

³⁵ Grant Agreement, Description of the Action, PART B, p.47.

2.1.10 Security Advisory Board (SAB)

The FERMI consortium will fully comply with their obligation to treat sensitive information in accordance with EU law and procedures. In this regard, particularly close attention will be paid to the full compliance with the requirements as described in “PROGRAMME SECURITY INSTRUCTION CONCERNING Horizon Europe Programme”³⁶ (Horizon Europe PSI) and the EU’s guide “How to handle security-sensitive projects: Projects with sensitive and classified information.”³⁷

Horizon Europe PSI stipulates that “[a] Project Security Officer (PSO) shall be nominated within the consortium to coordinate and promote actions in ensuring that the rules on the handling of classified information and the applicable security procedures are respected by the Beneficiaries of that consortium. Within the consortium the PSO shall normally be the first point of contact for the granting authority on security matters.”³⁸ In a similar vein the above-mentioned guide determines that “[i]f your project involves classified background or foreground information, you must appoint a project security officer (PSO). One PSO per project is sufficient. The PSO must have appropriate security clearance.”³⁹

Albeit FERMI will not produce or work with classified information in any way (this is explicitly clarified in section 5.2 of the Grant Agreement, which clearly states that the measures related to “[c]lassified [i]nformation” are “[n]ot [a]pplicable” to the project), the consortium is ready to go the extra-mile to guarantee all security-related aspects will be properly handled and to appoint a PSO. This commitment is made in the description of T1.4, which declares that the task leader will “assign a PSO for FERMI.”⁴⁰

Irrespective of the selection of a PSO, the EU’s guide “How to handle security-sensitive projects: Projects with sensitive and classified information” prescribes that “[a] security advisory board is needed if your project involves sensitive deliverables with security recommendation or classified background or foreground information.”⁴¹ There is no question that FERMI is obliged to fully comply with this requirement, considering that several project deliverables have been categorised as sensitive with security recommendation.

Section 5.1 of the GA explicitly mentions the exact audiences six such deliverables (the WP4 deliverables as well as D5.3 and D5.4) may be shared with. This list can be consulted as follows (adapted from the Grant Agreement):⁴²

Table 2: Sensitive information with security recommendation

Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access
D4.1: The FERMI integrated solution, 1 st version	INTRA	M18	EC, CONSORTIUM
D4.2: The FERMI integrated solution,	INTRA	M30	EC, CONSORTIUM

³⁶ The European Commission, *PROGRAMME SECURITY INSTRUCTION CONCERNING Horizon Europe Programme (SHORT TITLE: HORIZON EUROPE PSI)* (Brussels: European Commission, 2020).

³⁷ The European Commission, *EU Grants: How to handle security-sensitive projects. Projects with sensitive and classified information* (Brussels: European Commission, 2021), p.2.

³⁸ European Commission, *PROGRAMME SECURITY INSTRUCTION CONCERNING Horizon Europe Programme (SHORT TITLE: HORIZON EUROPE PSI)* (Brussels: European Commission, 2020), p.11.

³⁹ The European Commission, *EU Grants: How to handle security-sensitive projects. Projects with sensitive and classified information* (Brussels: European Commission, 2021), p.5.

⁴⁰ Grant Agreement, Description of the Action, PART A, p.7.

⁴¹ The European Commission, *EU Grants: How to handle security-sensitive projects. Projects with sensitive and classified information* (Brussels: European Commission, 2021), p.5.

⁴² Grant Agreement, Description of the Action, PART B, p.48-49.

final version			
D4.3: The FERMI disinformation watch, 1st version	INOV	M18	EC, CONSORTIUM, EU LEAs (Police and Border authorities from the EU)
D4.4: The FERMI disinformation watch, final version	INOV	M30	EC, CONSORTIUM, EU LEAs
D5.3: The FERMI final execution reports & assessments	IANUS	M36	EC, CONSORTIUM
D5.4: The FERMI Training curricula for officers & sessions' execution report	PUCF	M36	EC, CONSORTIUM, EU LEAs (Police and Border authorities from the EU)

Besides these six deliverables, there are further deliverables that have also been categorised sensitive, albeit the audience that is allowed to receive those is not specified in the Grant Agreement. Having said that, the aforementioned EU's guide "How to handle security-sensitive projects: Projects with sensitive and classified information"⁴³ stipulates that "[s]ensitive information with security recommendation [...] must not be downgraded, declassified or *further disseminated* [emphasis added], without the prior written consent of the originator (i.e. the authority under whose authority the information was created and classified)."

While the GA does not explicitly state that the further sensitive deliverables (unlike the six above-mentioned ones) have a security recommendation assigned to them, Art. 13.1 ("Sensitive information") clarifies that "[t]he parties must keep confidential any data, documents or other material (in any form) that is identified as sensitive in writing ('sensitive information') — during the implementation of the action [...]"⁴⁴ Accordingly, the FERMI consortium will avoid any security issues whatsoever by strictly limiting access to these deliverables to the EC and fellow consortium members. These further deliverables are part of the following list.

Table 3: List of further sensitive deliverables

Number and name of the deliverable	Name of lead participant	Date of production
D1.1: Overall Progress & QA Management, Innovation Management and Ethics Management Report	BPA	M12
D1.2: Overall Progress & QA Management, Innovation Management and Ethics Management Report	BPA	M24
D1.3: Overall Progress & QA Management, Innovation Management and	BPA	M36

⁴³ The European Commission, EU Grants: *How to handle security-sensitive projects. Projects with sensitive and classified information* (Brussels: European Commission, 2021), p.6.

⁴⁴ Grant Agreement, p.31.

Ethics Management Report		
D1.4: FERMI Data Management Plan	VUB	M6
D5.1: FERMI 1st execution reports - 1st version	SPA	M18
D5.2: FERMI 1st execution reports	SPA	M22
D7.1: H - Requirement No. 1	BPA	M3
D7.2: POPD - Requirement No. 2	BPA	M3
D7.3: AI - Requirement No. 3	BPA	M9

Given these sensitive outputs, the Grant Agreement declares that the consortium needs to create an SAB. More specifically, the above-mentioned task 1.4 commits the consortium to “ensure the formation of a[n] SAB, comprising both members from the FERMI partners and individuals outside the consortium. The SAB will be led by the PSO and will closely monitor the project's activities and provide guidance when needed.”⁴⁵

Thanks to the pre-coordination among FERMI partners in the proposal stage, this requirement has already been largely addressed. It has even been incorporated into the final version of the GA. Section 5 thereof addresses the entire “security” topic, which includes a set of remarks on the SAB. In particular, the SAB’s composition is being specified.

In full accordance with T1.4 the Grant Agreement clarifies that “[t]he SAB will include [...] listed representatives, that are part of the FERMI consortium.”⁴⁶ Besides mentioning these, namely Dr. Vassilios Chatzigiannakis, Tobias Mattes and Dr. Pirjo Jukarainen, the Grant Agreement also assigns the role of PSO to an employee of a consortium partner, namely Dr. Paraskevas Bourgos, a senior research and development project manager with INTRA.

Undoubtedly, the chair of the SAB as well as the members bring outstanding experience to the table, which makes them remarkably qualified to identify and mitigate any security-related issues. This is well documented in the remarks as follows (which are either direct quotes from the GA or closely adapted from it).

As far as the SAB’s chair is concerned, “Dr. Paraskevas Bourgos (M) [INTRA] [...] is a senior research and development project manager with significant experience in the EU funded projects in the area of innovative information and communication technologies. He graduated from the Computer Science Department of the School of Sciences and Engineering at the University of Crete in 2008. He received his MSc diploma in Parallel Distributed and Embedded Systems from the Department of Computer Science, Mathematics and Applied Mathematics and his PhD in the Development and Modelling of Embedded Systems from the University of Joseph Fourier, Grenoble, France in 2009 and 2013, respectively. Until 2014, he has also worked as a Postdoctoral associate at the Group of Distributed and Complex Systems in Verimag Laboratory, France. In 2019, he was certified as a Project Management Professional (PMP) by the Project Management Institute. Before joining INTRA, he had been working in WINGS ICT Solutions as a senior solution architect and project manager, involved in the technical project management of many EU funded as well as commercial projects. His main interests are in model-based development and performance analysis in heterogeneous and cyber-

⁴⁵ Grant Agreement, Description of the Action, PART A, p.7.

⁴⁶ Grant Agreement, Description of the Action, PART B, p.49.

physical systems, smart system integration and robust systems with cognitive capabilities and advanced automation.”

In full accordance with the above-mentioned requirement that “[t]he PSO must have appropriate security clearance,” Dr. Bourgos “has received personnel security clearance in 2022 from the National Ministry of Defense at EU SECRET and NATO SECRET level, and he has been working on data privacy and network security in numerous research and innovation projects, verifying his capability to act as PSO for [the] FERMI project.”⁴⁷

Again, the further SAB members are equally qualified to monitor security-related developments, which is clearly corroborated by their expertise that is summarised in the following set of remarks.

“Dr. Vasilis Chatzigiannakis has received his PhD and his bachelor’s degree in electrical and computer engineering, both from the National Technical University of Athens (NTUA). He is currently the Technical Director at ITML. He has also worked in the Network Operations Center in NTUA and Netcompany-Intrasoft SA. Dr. Chatzigiannakis has more than 20 years of experience in technical project management, advanced Computer Science topics, numerous programming languages, development tools and frameworks. His research focuses on network security and data protection & privacy solutions. Due to the nature of his work he is used to work with information security and sensitive information.”

Tobias Mattes is an experienced Police Officer and researcher. He has been a Bavarian State Police (BSP) Officer since 1999. Between 2007 and 2009 he completed his studies at the University of Applied Sciences for Public Services in Bavaria (Department of Police Management and Policing). Up until 2013 he was part of the BSP’s middle management and the Liaison Officer US-Army USAG-Bavaria. He was involved in BSP’s personnel development until 2016 and later studied at the German Police University (Deutsche Hochschule der Polizei, DHPol), taking his final exams in 2018 with a focus on cybercrime, radicalisation and extremism. Currently, he is a lecturer at the Department of Criminology of the University of Applied Sciences for Public Services in Bavaria (responsible for cybercrime, IT, data protection, data security), as well as a scientific researcher participating in the management and coordination of several H2020 EU projects with a focus on cybercrime, AI driven policing approaches, radicalisation and counterterrorism. Since 2019 he has held the rank of Chief-Superintendent in the Bavarian State Police. He is currently a PhD Candidate at the German Police University in the field of radicalisation and counterterrorism.

Mrs. Jukarainen is holding a PhD in Public Administration and is working as a project manager and lecturer at the Police University College of Finland. She is an adjunct professor at Tampere University, Finland. Her recent research has focused on preventative issues, engaging communities in safety and security work, security risk analysis, community policing and intelligence-led law enforcement. She is also used to and experienced in dealing with sensitive and security related information and documents. After completing EU funded Horizon 2020 projects such as Unity - Community Policing, MINDb4ACT on radicalisation and extreme violence, and BuildERS on building European communities’ resilience and social capital in crisis, she has been involved in a project funded by the Internal Security Fund on critical infrastructure.⁴⁸

As impressive as this GA-derived list of SAB members is and albeit a lot of progress has already been made in the effort to fully meet the Grant Agreement’s requirement to create a perfectly qualified and reliable SAB, there was one outstanding issue concerning the board’s composition. As mentioned above, T1.4 lays out that the SAB should include “both members from the FERMI partners and individuals outside the consortium”,

⁴⁷ Grant Agreement, Description of the Action, PART B, p.49.

⁴⁸ Grant Agreement, Description of the Action, PART B, p.50.

whereas the above-mentioned SAB members that are explicitly alluded to in the GA “are part of the FERMI consortium,”⁴⁹ as clarified in the GA’s section 5.

The need to bring in external experts is a reasonable requirement to avoid the pitfalls of group think. Against this backdrop, the FERMI consortium is very proud to have been able to recruit Mrs. Léonie Bouwknecht as a non-consortium SAB member. Léonie Bouwknecht is an Operational Specialist working in the Unit Limburg of the National Police of the Netherlands. With almost 25 years of experience within many different operational teams, mostly in the field of criminal investigation, she is seen as an expert in addressing issues by using a comprehensive strategy. Currently she is working as a strategic advisor on the following topics: organised crime, digitalisation and cybercrime, care and safety and international cooperation. A further field of expertise is arts-related crimes.

Mariana A. Risetto is a lawyer who graduated from the University of Buenos Aires (Argentina) and holds an LL.M. in International Legal Studies from the University of Vienna (Austria). The focus of her professional legal career has been mainly on the public (international) sector as a legal consultant with key strengths in international institutional law, and international and European data protection, IT and privacy law. Since February 2019 she has served as a research associate at the Department of Innovation and Digitalization in Law (University of Vienna) and is supporting lead in several European Horizon 2020 security (e.g. ODYSSEUS, PERIVALLON) and healthcare research projects (VirtualBrainCloud, BIOMAP). As a privacy engineer, she provides support and advice on privacy and data security, in particular in the field of artificial intelligence and new technologies. She is also an active member EU funded research projects’ EABs.

Thanks to the recruitment of Léonie Bouwknecht and Mariana A. Risetto the FERMI SAB has also achieved full gender balance, as it encompasses three female and three male members (including the chair).

This leaves us with the following list of SAB experts:

Table 4: List of SAB experts

SAB Expert	Position in SAB	Nationality	Profession	Areas of Competence
Dr. Paraskevas Bourgos	Chair	Greek	Senior Research and Development Project Manager	Model-based development and performance analysis in heterogeneous and cyber-physical systems, smart system integration and robust systems with cognitive capabilities and advanced automation
Dr. Vassilios Chatzigiannakis	Member	Greek	Chief Technology Officer	Information security, Cybersecurity, network security, data security
Tobias Mattes	Member	German	Police Officer and Researcher	Information security, Cybercrime, AI driven policing approaches, Radicalisation and

⁴⁹ Grant Agreement, Description of the Action, PART B, p.49.

				Counterterrorism
Dr. Pirjo Jukarainen	Member	Finnish	Researcher	Communications, Crisis preparedness, Policing
Léonie Bouwknecht	Member	Dutch	Operational Specialist	Organised crime, Digitalisation and cybercrime, care and safety and international cooperation
Mariana A. Risetto	Member	Argentinean/ Austrian	Research Associate and Privacy Engineer	Privacy Engineering, Data Security, Data Protection in law enforcement

Additional external experts might be recruited later on, depending on the workload and the necessity to consult non-consortium members to get some outside expertise.

Having said that, the workload (see below) seems to be manageable for the time being, especially for a group of highly distinguished experts and the risk of biased security assessments has been successfully mitigated due to the selection of SAB members that are not too intimately involved in the project. In this respect, the choice of the SAB chair as well as the three inner-consortium members speaks for itself. Despite their affiliations with consortium partners, none of these experts will be involved in the day-to-day management of FERMI and may even entirely limit their contribution to monitoring security proceedings.

The chair, Dr. Paraskevas Bourgos, is a case in point. His role in INTRA as a senior research and development project manager notwithstanding, INTRA's contribution to FERMI (as long as the activities in question do not directly concern the work of the SAB) will be managed by a different group of experts. The same applies to the role of Dr. Vassilios Chatzigiannakis and the division of labour within the partner he is affiliated with, namely ITML. Tobias Mattes, who is affiliated with BPA, is a police officer who is involved in BPA's research and teaching activities but will mostly focus on ensuring FERMI's compliance with security standards. Equally, Dr. Pirjo Jukarainen will not be responsible for project management proceedings either other than those related to the SAB.

To further ensure that the SAB can work as independently as possible, all communication between the SAB's chair and its members will take place outside of the consortium's regular communication chains. So instead of exchanging emails via the FERMI mailing list, the SAB members will always directly communicate with one another.

As far as the SAB's exact role and responsibilities are concerned, it is explained in the Grant Agreement that "[t]he SAB will review the project deliverables, to assess whether they include any security sensitive information and to propose timely measures for preventing the misuse of such information."⁵⁰ In the context of T1.4, it is further clarified that "[t]he SAB [...] will closely monitor the project's activities and provide guidance when needed."⁵¹ These descriptions give a very compelling overview of the SAB's duties.

The in-depth review of the project deliverables is a hugely important measure to ensure that all deliverables are submitted in good quality (which is the job of the peer reviewers) and in full compliance with ethical and legal norms and rules (which is the job of the EAB reviewers). The SAB review of security-relevant aspects is one further step to guarantee that the deliverables can be submitted as they are.

⁵⁰ Grant Agreement, Description of the Action, PART B, p.49.

⁵¹ Grant Agreement, Description of the Action, PART A, p.7.

Such reviews will be conducted before any deliverable will be submitted. This is fully in line with the Grant Agreement’s wording as quoted above, which is highly inclusive. The assigned task to “review the project deliverables” covers all such outputs.

As far as those deliverables that have been categorised public are concerned, the SAB will, as the wording above implies, ensure that those do not include any sensitive information, let alone any statements that would require their classification. As far as those deliverables that have been categorised sensitive are concerned, the key challenge appears to be to ensure that those do not include any information that should not be shared with the assigned target groups that have been cleared to be given access. For example, D4.3 and D5.4 can be shared with the “EC, CONSORTIUM, EU LEAs (Police and Border authorities from the EU)”, unlike other sensitive deliverables that are not allowed to be distributed amongst non-consortium members other than the EC. The security check would then conduct an assessment as to whether both deliverables – before they are being submitted – can be truly shared with EU LEAs or whether they contain security-relevant material that no non-consortium member should have access to.

Similarly, all further sensitive deliverables ought to be checked to ensure that the classification as sensitive is still valid in the sense that the sensitive information – in accordance with the EU’s classification guidelines – do not include proceedings which would require the deliverables classification.

Obviously, the further obligation (the one that is also mentioned in the Grant Agreement but not related to reviewing project deliverables from a security standpoint) that the “[t]he SAB [...] will closely monitor the project’s activities and provide guidance when needed”⁵² is a lot more abstract. However, it alludes to an important focal point, namely the project’s activities that may require security checks or that at least need to be elaborated on from a security standpoint although they are not necessarily embedded in the deliverables.

(Non-deliverable) publications are a case in point. According to the GA, the FERMI consortium is, among other things, obliged to publish six peer-reviewed and six non-peer-reviewed journal articles. It would surely be an overreach to have the SAB review each and every draft that addresses the project’s topics and is submitted for publication irrespective of its content. For example, it would make very little sense to have the SAB check literature reviews that simply summarise what has already been made publicly available beforehand. Neither would it be reasonable to require assessments of legal norms and rules that are also freely available to anybody to be run by the SAB before submission.

Some publications, however, certainly require such a review. Any article that describes sensitive technical proceedings like the ones the consortium will be working on within the framework of WP4 and WP5 needs to be checked to avoid that sensitive pieces of information are released. The same applies to any draft publication (whatever the format is) that gets into any other (non-technical) topic or insight that may be part of the sensitive deliverables. In the event it is unclear whether a security review of a draft publication is necessary, the SAB itself should decide whether the relevant material requires a security check.

Other than its review duties, the SAB should also be up-to-date on FERMI’s technical proceedings to get a clear understanding of the tools that are being developed and the potential implications thereof. The technical partners should keep the SAB in the loop on the key steps they are undertaking so the SAB can provide counsel and, if deemed necessary, express concerns about the consequences of using the tools from a security standpoint. To fully ensure that the tools’ use within the project’s framework does not violate any security guidelines and standards one SAB representative will take part in each pilot session to monitor the proceedings. The SAB will – if necessary – also express any such concerns about any other security-relevant development.

The SAB will also ensure that the technical environment and tools for the project management and internal communications do not compromise the data security and communication needs of different project partners,

⁵² Grant Agreement, Description of the Action, PART A, p.7.

especially concerning the potential end-users. This includes a) videoconferencing channels, b) document repositories/cloud services and workplaces, and c) possibly also the FERMI platform, including the training dimension. As a first step, the PC and the SAB will inquire into the tools that the WPLs and further organisers of online meetings prefer to use and provide an update on the envisaged repository. The SAB will then run the result by the partners, especially on the LEA side. The latter can express any severe objections they might have. This effort will ensure that the within-consortium communication is feasible and that all project partners can safely participate in the project.

The chair and the SAB members will closely work with the consortium to address any security-related issues, if they arise, so the consequences thereof can be mitigated and eventually fully resolved. To ensure all of these commitments can be met the SAB pledges to hold biannual gatherings to discuss outstanding security issues (and to gather whenever ad-hoc meetings are required) and to properly document those.

To sum up and conclude, the SAB commits to the following list of duties:

- Review the project deliverables from a security standpoint
- Review draft publications that could possibly reveal sensitive information
 - If necessary, provide counsel on whether a draft publication requires a security review
- If necessary, provide counsel on the technical tools that are developed in the FERMI project from a security standpoint
 - One SAB representative will take part in each pilot session to monitor compliance with security proceedings
- Ensure that the technical environment and tools for the project management and internal communication do not compromise the data security and communication needs of the partners, especially on the LEA side
- Provide counsel on any other security-related issue that may arise throughout the project's duration
- Identify security issues that require action and help the consortium mitigate the implications thereof so they can be fully resolved
- Have biannual meeting plus further meetings on an ad-hoc basis whenever necessary
- Properly document all discussions in the form of key takeaways and action points that will be made available to all SAB members shortly after all meetings

2.1.11 Ethics Advisory Board (EAB)

Unlike other committees and boards, the creation of an EAB does not appear to be explicitly required by the GA. However, the Grant Agreement does emphasise the importance of ensuring full compliance with ethics and data protection-related proceedings, most notably in T1.5, which obliges the consortium to the “[c]ontinuous monitoring of research ethics,” as explained above.

The description of the task implies, albeit this is not directly mentioned, that the creation of an EAB may surely be a helpful step. In this respect, the above-mentioned wording that aims to conceptualise an “ethics compliance protocol for the research lifecycle of FERMI” (also referred to as “an internal protocol for ethical procedures”), which will “ensure adequate ethical standards are met through the research process” speaks for itself.

In other words, a whole set of criteria for the entire consortium to comply with throughout all research activities is to be laid out. To ensure full compliance with the envisaged protocol it is also stipulated that “[t]his task will organise the internal monitoring of the implementation of the ethics protocol by the consortium,” as the task’s

title implies. “The evaluation of this monitoring exercise will be reported during the project’s interim and final reports.”⁵³

Arguably, this is a highly demanding process that requires that certain ground rules are not just presented in the first place but which also commits the task leader and task partners to overseeing the whole consortium’s compliance with those and to assessing the outcome thereof. The creation of an EAB to coordinate between the task leader, the task partners and – if necessary – all other consortium partners, surely is a proper step to facilitate this process and to provide the aspired results.

As explained above, considering that VUB is entrusted with leading this task, they are a self-evident candidate for chairing the EAB. Brief consultations between VUB, KU Leuven in their capacity as Legal and Ethics Advisors and BPA in their capacity as coordinator have helped the three partners reach an agreement that does assign the role of chair to VUB with KU Leuven and BPA supporting the EAB’s work.

Accordingly, the EAB will be chaired by VUB’s key contact persons for and contributors to the FERMI project, namely Dimitra Markopoulou and Vagelis Papakonstantinou, which also ensures full gender parity on the chair level. Further information on both chairpersons as well as further members of the EAB – that have also been picked on the basis of full gender parity – can be found as follows:

Table 5: List of EAB experts

EAB Expert	Position in EAB	Nationality	Profession	Areas of Competence
Dimitra Markopoulou	Chair	Greece	Senior Researcher	Data Protection and Privacy, Cybersecurity, Information Technology Law, Telecommunications Law, Intellectual and Industrial Property, as well as Business Law
Vagelis Papakonstantinou	Chair	Greece	Professor	Data protection, ethics in research, Technology law, cybersecurity
Flavia Giglio	Member	Italian	Researcher	Data protection, cybercrime, cybersecurity, criminal law
Sven-Eric Fikenscher	Member	Germany	Senior Researcher	Ethics in research and security research.

The chairs as well as the members of the EAB, which, again has achieved full gender parity across the board and on all levels, are highly qualified to monitor the project’s compliance with ethical rules (and to conceptualise those in the first place). This is clearly demonstrated by the CVs of the above-mentioned individuals.

Dimitra Markopoulou is a senior researcher at the VUB Cyber and Data Security Lab. She holds a Bachelor in Law (LLB) from the Democritus University of Thrace-Faculty of Law, and acquired her LL.M. in European

⁵³ Grant Agreement, Description of the Action, PART A, p.7.

Law and Policy (with an emphasis on Telecommunications Law) from the University of Manchester. She is a member of the Athens Bar Association and is a co-founder of MPlegal, a niche technology law firm in Athens.

Her fields of expertise include data protection and privacy, cybersecurity, Information Technology Law, Telecommunications Law, Intellectual and Industrial Property, as well as Business Law. She is a PhD candidate with a focus on cybersecurity law and policy. Since 2018, she has participated as a partner through VUB's CDSL in EU-funded research projects and has provided her expertise on ethics and data protection issues. From 2019 until today she has participated as an independent ethics advisor in an EU H2020 project. Her active involvement in the fields of both personal data and research ethics is expected to contribute to the project's compliance with data protection legislation, as well as with the EC requirements on ethical matters.

Vagelis Papakonstantinou is a Professor on Personal Data Protection Law at the Faculty of Law & Criminology of VUB, focusing also on cybersecurity, Intellectual Property, and the broader topic of technology regulation. He works through CDSL, where he is scientific coordinator, as well as through VUB's Research Group on Law Science Technology & Society (LSTS) and the Brussels Privacy Hub.

Since the early 2000s Vagelis Papakonstantinou has participated in the law-making committees for the release of all major EU, Council of Europe and Greek laws and regulations on personal data protection (the Council Framework Decision 2008/977/JHA, the EU PNR Directive, Convention 108+, the GDPR, the Police and Criminal Justice Data Protection Directive, Greek law n.4624/2019). For the period of 2016-2021 he has been a member (alternate) of the Hellenic Data Protection Authority. In the past, he has been a member of the Board of Directors of the Hellenic Copyright Organisation (for two terms).

Flavia Giglio is a Research Associate at the Center for IT & IP Law (CiTiP) of KU Leuven. She works in the cluster "Cybersecurity & Cybercrime", where she focuses on projects concerning the intersection between technological developments, criminal law and national security. In her role as researcher at CiTiP, she has worked on projects and Horizon Europe proposals dealing with cybersecurity of critical infrastructures, the balance between data protection and law enforcement's objectives in fighting transnational forms of crime, and the protection of personal data in pursuing national security objectives. She also contributed to studies commissioned by EU institutions and bodies concerning the EU framework on privacy and data protection in the law enforcement domain. As a result, she continuously focused on the study of both the GDPR and the Law Enforcement Directive (2016/680), and she has an in-depth understanding of the privacy and data protection principles governing the action against crimes and the standards with which the FERMI project must comply when it comes to the protection of personal data.

Sven-Eric Fikenscher is a senior researcher with BPA. In the context of his involvement in the management of numerous projects in which BPA has participated as a beneficiary (among other things as WP and task leader) and also as a coordinator, he has done substantial work on ethics. Currently, this is exemplified by his role as a member of the EAB of another Horizon project, CC-DRIVER, which seeks to understand the drivers of cybercriminality and researches methods to prevent, investigate and mitigate cybercriminal behaviour. As a result, he has first-hand experience in overseeing the handling of large amounts of (online and crime-related) data from an ethics perspective.

Moreover, he was intimately involved in the across-the-board ethics review of PROPHETS, a further Horizon project, which was coordinated by BPA. The informed consent forms and information sheets that were produced within the framework of PROPHETS have served as role models for a project supported by the Internal Security Fund-Police that is presently underway, called PROTECTOR, which examines and attempts to advance the security of places of religious significance, especially amidst threats posed by hate crimes and terrorism. Interestingly, such hate crimes and terrorist offences against religious sites are often-times rooted in conspiracy theories and fake news propaganda along the lines of FERMI's focal points. He has worked with

EABs and applied draft informed consent forms and information sheets to BPA’s research activities in several further EU-funded projects too.

One of the best ways to guarantee that the entire consortium actually is in full compliance with the to-be-developed ethics protocol is to have the EAB review all project deliverables from an ethics and data protection standpoint. Accordingly, each and every deliverable will be checked by at least one EAB member before submission.

Moreover, major research efforts, especially those that include the use of sophisticated technology with possibly huge ethics implications may require pre-consultations with the EAB. Therefore, the EAB will be informed about all such major developments so the chairs and the members can identify any ethics and data protection-related pitfalls in due course. In the event such shortcomings are detected the EAB will provide counsel on how to mitigate the problems that have arisen so these can be successfully addressed and fully resolved.⁵⁴ To facilitate the achievement of these objectives the EAB pledges to meet regularly, at least biannually and on an ad-hoc basis, whenever required. The outcome of such gatherings will be properly documented.

As a result, the EAB commits to the following list of duties:

- Draft an ethics protocol
- Have all partners sign the ethics protocol
- Monitor the consortium’s compliance with the ethics protocol
- Review all deliverables to ensure their compliance with the EU’s ethics and data protection norms, rules and laws

⁵⁴ So far this includes the following ethical and legal requirements that have been identified amidst an ethics review and that are to be addressed in the WP7 deliverables on ethics (Grant Agreement, Description of the Action, PART A, p.24-25):

- “The procedures and criteria that will be used to identify/recruit research participants must be submitted as a deliverable before the start of the relevant activities.
- The informed consent procedures that will be implemented for the research participants must be submitted as a deliverable before the start of the relevant activities.
- Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) must kept on file (submit confirmation) and provided upon request.”
- “Clarification how all of the personal data that will be processed are relevant and limited to the purposes of the research project (in accordance with the ‘data minimisation ‘principle) and in conformity with the EU Directives 2016/679 and 2016/680 must be submitted as a deliverable before the start of the relevant activities.
- A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects must be submitted as a deliverable before the start of the relevant activities.
- A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing must be submitted as a deliverable before the start of the relevant activities.
- A detailed analysis of how the proposed personal data collection and processing and behavioural profiling activities complies with EU Directive 2016/680 needs to be submitted as a deliverable. The analysis needs to include aspects related to the principles related to processing of personal data, time limits for storage and review, verification of the quality of personal data, automated individual decision-making, and the rights of the data subjects.”
- “A detailed explanation on the measures taken to prevent, avoid and mitigate potential bias, discrimination and stigmatisation in input data and algorithm design and outcomes must be submitted as a deliverable before the start of the relevant activities.
- A detailed explanation on how the research participants and/or end-users will be informed about: (1) their interaction with an AI system/technology (if relevant); (2) the abilities, limitations, risks and benefits of the AI system/technique; (3) the manner in which decisions are taken and the logic behind them (if relevant) must be submitted as a deliverable before the start of the relevant activities.
- A detailed explanation on how humans will maintain meaningful control over the decision-support capabilities of the overall platform must be submitted as a deliverable before the start of the relevant activities.”

- Provide counsel on all aspects of the project that are related to ethics and data protection, whenever necessary
- Identify ethics and data protection issues that require action and help the consortium mitigate the implications thereof and eventually resolve them
- Have regular meetings biannually and whenever ad-hoc meetings are necessary
- Properly document all discussions in the form of summaries, including key takeaways and Action Points that will be drafted by the chairs and made available to all SAB members shortly after all meetings

2.2 Work Package Management

FERMI is broken into six Work Packages with each WP containing a set of associated and interrelated tasks, accompanied by WP7 which focuses on ensuring that the project complies with its ethical requirements. The overall WP plan has been agreed by all parties and lays the ground for implementing a commonly agreed upon work plan along the lines of the project’s deliverables and milestones.

Each WP will be led and co-ordinated by a Work Package Lead. It is the responsibility of each WPL to coordinate the activities in the respective WP (for the detailed responsibilities see section 2.1.8). A summary of the leads for each WP and tasks is outlined in the table below:

Table 6: WP overview

WP#	Title	Partner	PMs	Start	End
WP1	Project and Technical Management	BPA	55	M1	M36
WP2	FERMI touchbase: Societal landscape, Technology convergence and end users' needs	INTRA	57	M1	M6
WP3	Technology Offerings	UCSC	114	M6	M30
WP4	User Interfaces and Platform Integration	ITML	79	M9	M36
WP5	Pilot Demonstration and Validation Campaigns	IANUS	138	M9	M36
WP6	Outreach management, exploitation and maximization of digital trust	LC	101	M1	M36

2.3 Project deliverables

The project includes a list of deliverables certifying the project’s achievements. All project deliverables are associated with a specific WP task. It is the responsibility of the lead beneficiary to co-ordinate the drafting of the deliverable and to ensure the inputs of other partners where necessary. Each partner should apply its individual quality procedures in order to self-assess their own contribution in addition to the internal review process (see section 4.1).

A deliverable template has been developed and will be used for all project deliverables, starting with this one. The table below provides an overview of all deliverables. The scheme indicates the deliverable number, the title, the WP number, the lead beneficiary, the type of deliverable, the dissemination level as well as the due date.

Table 7: List of project deliverables

Del. No.	Title	WP No.	Lead Beneficiary	Type	Dissemination Level	Due Date (in months)
D1.1	Overall Progress & QA Management, Innovation Management and Ethics Management Report	1	BPA	Report	SENSITIVE	M12
D1.2	Overall Progress & QA Management, Innovation Management and Ethics Management Report		BPA	Report	SENSITIVE	M24
D1.3	Overall Progress & QA Management, Innovation Management and Ethics Management Report		BPA	Report	SENSITIVE	M36
D1.4	FERMI Data Management Plan		VUB	Report	SENSITIVE	M6
D1.5	FERMI Project Management Playbook		BPA	Report	PUBLIC	M2
D2.1	FERMI starting point package	2	INTRA	Report	PUBLIC	M6
D3.1	Fermi technology facilitators package 1st Version	3	UCSC	Report	PUBLIC	M16
D3.2	Fermi technology facilitators package		UCSC	Report	PUBLIC	M30
D3.3	FERMI behaviour analyses and community resilience facilitators package 1 st Version		BIGS	Report	PUBLIC	M16
D3.4	FERMI behaviour analyses and community resilience facilitators package		BIGS	Report	PUBLIC	M30
D4.1	The FERMI integrated solution 1st version	4	INTRA	Report	SENSITIVE	M18
D4.2	The FERMI integrated solution		INTRA	Report	SENSITIVE	M30
D4.3	The FERMI disinformation watch 1st version		INOV	Report	SENSITIVE	M18
D4.4	The FERMI disinformation watch		INOV	Report	SENSITIVE	M30
D5.1	FERMI 1st execution report	5	SPA	Report	SENSITIVE	M18
D5.2	FERMI 1st execution reports		SPA	Report	SENSITIVE	M22
D5.3	The FERMI final execution reports & assessments		IANUS	Report	SENSITIVE	M36
D5.4	The FERMI Training curricula for officers & sessions' execution report		PUCF	Report	SENSITIVE	M36
D6.1	The FERMI outreach management facilitators package	6	LC	Report	PUBLIC	M4

D6.2	FERMI outreach and collaboration management report 1 st Version		LC	Report	PUBLIC	M18
D6.3	FERMI outreach and collaboration management report		LC	Report	PUBLIC	M36
D6.4	FERMI Market analyses and business modelling towards exploitation		INTRA	Report	PUBLIC	M36
D7.1	H - Requirement No. 1	7	BPA	Ethics	SENSITIVE	M3
D7.2	POPD - Requirement No. 2		BPA	Ethics	SENSITIVE	M3
D7.3	AI - Requirement No. 3		BPA	Ethics	SENSITIVE	M9

2.4 Project Milestones

To assess the overall progress and coherency of the project, six main project milestones have been defined. The assessment of these milestones (see Table 8 below) will be based on the relevant project deliverables produced before the respective milestone date.

Table 8: Project milestones

Milestone No.	Milestone Name	WP No.	Means of Verification	Due Date (month)
1	Project's baseline	2,6	FERMI starting point package, Project's digital identity ready; Thorough outreach plan ready	8
2	Innovation Flame	3,4	Preliminary versions of all technologies and modules, FERMI services; MVP	12
3	Innovation Fire	3,6,4	1st complete versions of all technologies and modules & integrated FERMI framework, 1st reports on outreach and collaboration activities	18
4	Demonstration Flame	5,3,4	1st round of pilots executed	24
5	Demonstration Fire	5,3,4	Final versions of all technologies and modules & Integrated framework, 2nd round of pilots executed	30
6	Pathways towards holistic approach against D&FN	5,3,6,4	The FERMI final solution, Overall Impact assessment in place	36

3 Project Communication

3.1 Project Meetings

The Consortium met at the start of the project (M1) at the coordinator’s premises in Fürstenfeldbruck. Further physical meetings of the whole consortium are envisaged twice a year, or on an ad hoc basis as requested. The meetings take place alternately at the different partners’ premises. Prior to every meeting, the host of the meeting circulates an agenda (in collaboration with the coordinator) and location information within the consortium to allow timely and good preparations by all participants as well as smooth travel and logistical organisation.

Table 9: Indicative timetable of physical project meetings

No	Meeting Type	Month	Date	Hosting Partner	Location
1	Kick off Meeting	M1	October 2022	BPA	Fürstenfeldbruck
2	Consortium Meeting	M7	April 2023	TBD	TBA
3	Consortium Meeting	M12	October 2023	TBD	TBA
4	Consortium Meeting	M18	March 2024	TBD	TBA
4	Rehearsal & Mid Term Review	M19	April 2024		Brussels
5	Consortium Meeting	M24	October 2024	TBD	TBA
6	Consortium Meeting	M30	April 2025	TBD	TBA
7	Consortium Meeting & Final Review	M36	October 2025		Brussels

3.2 Content Management System (CMS)

The content management system (CMS) is an open platform for digital team collaboration, which is used to facilitate the sharing of information and overall project management.

The Service Centre of the Free State of Bavaria (IT-DLZ) provides a central infrastructure for the exchange of data with external partners and agencies outside the Bavarian public authority network. For this purpose, the IT-DLZ uses OwnCloud and thus provides a web interface for the exchange of data and user administration, which is connected to a MySQL database in the background.⁵⁵

For the duration of the project, a FERMI OwnCloud installation is envisaged to be the main tool for online collaboration and serve as document repository. (So far, no partner has expressed concerns over the use thereof). BPA is responsible for setting up the CMS and maintaining it, along with contribution of all partners. The access to the repository will be limited to authorised consortium users with the appropriate access credentials (username and personalised password).

⁵⁵ Landesamt für Digitalisierung, Breitband und Vermessung, *IT-Dienstleistungszentrum des Freistaats Bayern, Datenaustausch mit Externen* (Landesamt für Digitalisierung, Breitband und Vermessung, 2022). Available at: http://www.it-dlz.bybn.de/dienstleistungen/datenaustausch_owncloud/index.html.



Figure 1: Content Management System - Login page

The collaborative workspace captures the day-to-day activities of the project and ensures the easy and secure access to the project's documents which will be collaboratively processed by the consortium partners including templates, meeting minutes, deliverables, presentations etc. Every partner has full permission to read and write within the shared FERMI folder.

The project online repository has been structured in multiple sub-folders for easier navigation (Deliverable Tracker, DoA, Project Meetings, Templates etc.). In addition, each WP has a dedicated folder which shall be used by all partners for online collaboration within the WP teams. It is the responsibility of the WPL to manage the structure of their respective folder.

The first level of the archive structure follows:

- Deliverable Tracker
- DoA
- Project Meetings
- Templates
- WP1
- WP2
- WP3
- WP4
- WP5
- WP6
- WP7

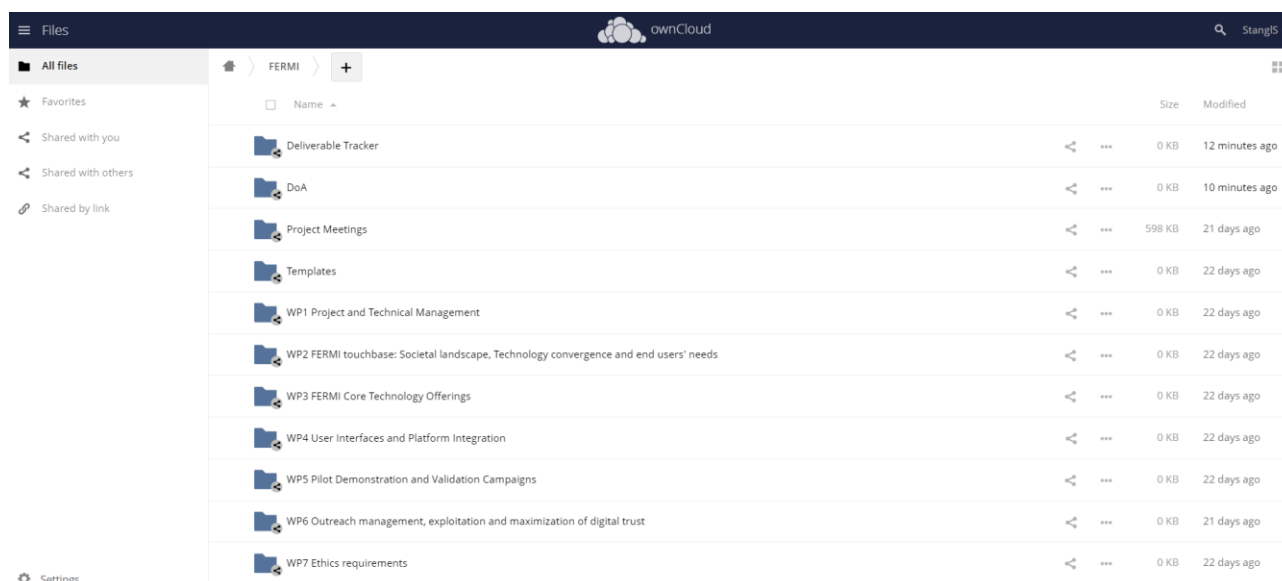


Figure 2: First level structure

3.3 Communication tools

Effective and efficient communication among project partners is fundamental in achieving the best results and must therefore be carried out by all consortium members. A dedicated mailing list (fermi@lists.itml.gr) has been set up, which will be updated and supplemented over the course of the project (WP-specific mailing lists as well as others will be created where needed). E-mail correspondence is the main communication route of the project for the organisation of project activities, project-related announcements or general support. Mailing list membership will be granted or revoked by the mailing list owner. Communication will be inclusive and copies of correspondence relevant to the project will be sent to all relevant members.

So far, no partner has expressed concerns over the use of Microsoft Teams as internal communication tool for all conference calls (WP, Steering Committee and DKMC) to discuss progress of work packages and tasks as well as other relevant topics.

3.4 Visual identity

The visual identity of a project is important to promote consistency and to make it unique and instantly recognisable. A coherent image improves the communication within the consortium and with the European Commission and is further built through the attendance to conferences, workshops and meetings with external stakeholders.

The project's visual identity of FERMI is constructed around the FERMI logo. The logo was put to a vote at the beginning of the project and was selected according to the majority principle. The final version of the project logo is presented below. It should be put on all communication products and dissemination materials.



Figure 3: Fermi logo

The corresponding colour scheme for the project is depicted below:

R=0 G=0 B=0



R=225 G=225 B=195



In addition, various templates have been developed to ensure a high quality of all the project's documents and to support a coherent visual identity, including:

- Deliverable template
- PowerPoint template
- Reporting templates
- Meeting minutes template

All FERMI templates are available for download on the shared online repository. These templates should be used by all partners for the entire duration of the project.

Further documentation and dissemination material tailored to external stakeholders will be created for various communication purposes, while always maintaining the visual identity of the project.⁵⁶

⁵⁶ A central external communication tool will be the FERMI website, available at <https://fighting-fake-news.eu/>. Further external tools include the FERMI social media profiles. For more information, please see the communication starter package (attached to D6.1).

4 Monitoring, Reporting and Quality Assurance

As explained above, quality management includes the following set of guidelines “(i) control actions planned; (ii) time schedules; (iii) requirement specifications and quality objectives will be clearly defined and documented; (iv) responsibilities and authorities will be clearly defined; (v) development, quality, testing, configuration, acceptance and maintenance plans will be defined and controlled; (vi) agreed definitions of procedures for acceptance and quality control will be established; and (vii) appropriate tools for planning, monitoring and progress reporting will be proposed.”⁵⁷

These cornerstones have informed the FERMI consortium’s – in particular the PC’s and Quality Manager’s – approach to overseeing key project proceedings, mostly the deliverables but also the overall progress that is being made, which will be part and parcel of the internal progress reports as well as periodic progress reports.

4.1 Deliverable submission process

All deliverables are subject to an internal peer review before their final submission, which presumably constitutes the project’s major control action and meets the GA’s requirement that “all the [...] partners will have to enrol in a peer review.”⁵⁸ Accordingly, two peer reviewing partners are appointed from within the consortium for each deliverable, which clarifies the responsibility issue. The peer reviewers have been selected by the PC and the quality manager (INTRA) according to their expertise. The FERMI Deliverable Tracker (see Annex A) has been shared with the consortium at the Kick-off meeting and is further stored in the CMS.

With the aim of achieving high quality standards in the deliverables, the project follows a review procedure to guarantee the quality, completeness, and consistency of each document. The deliverables must be delivered on time and thus they need to meet internal deadlines in order to allow for sufficient time to prepare the table of contents (ToC), developing the initial versions, performing internal reviews and updates, as well as a final review.

The designated peer reviewers must have (to a professional standard) objectivity, ideally without heavy involvement in the deliverable preparation. It will be their responsibility to review the deliverable in accordance with the criteria identified in the review template (see Annex B). All reviewers are asked to evaluate the deliverables by completing the template, which includes a set of guiding questions inquiring into the comprehensiveness and plausibility of the to-be-reviewed draft. This is fully in line with numerous of the above-mentioned criteria such as defining “quality objectives”, “agreed definitions of procedures for acceptance and quality control” as well as presenting “appropriate tools for planning, monitoring and progress reporting.”

Moreover, the “time schedules” as well as the “responsibilities and authorities” have indeed been “clearly defined.” More specifically, the lead beneficiaries are asked to share the ToC with the quality manager (INTRA), the coordinator (BPA), the key contributors and the assigned peer reviewers two and a half months prior to the deliverable’s submission. It will also be the responsibility of the author(s) to ensure the draft of the deliverable is shared with the peer, the EAB and SAB reviewers at least a month before the deliverable is due for final submission. Reviewers will provide feedback within one week after the date they receive it. The lead beneficiary will have one week to revise and finalise the report and to send it back to the coordinator and the quality manager no later than 15 days prior to the submission deadline. The PC will create the final PDF version to be submitted to the Portal.

⁵⁷ Grant Agreement, Description of the Action, PART A, p.6.

⁵⁸ Grant Agreement, Description of the Action, PART A, p.6.

In case any delay is foreseen, the PC must be notified as soon as possible and the deliverable leader should suggest a mitigation plan as early as the risk of delay is recognised to decrease the impact it may have on the project.

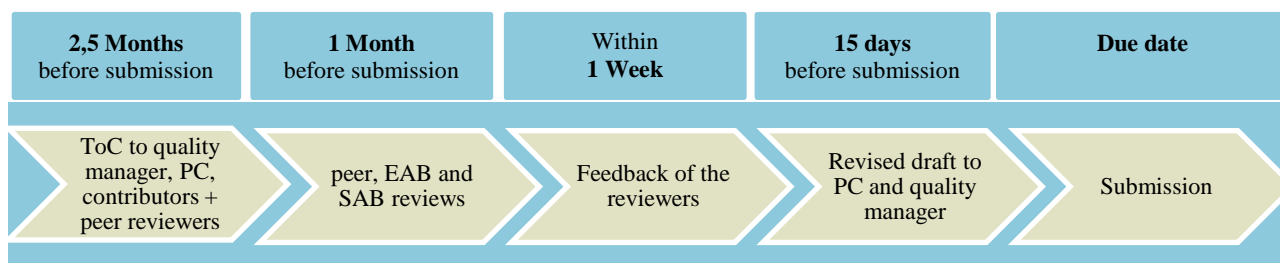


Figure 4: Deliverable submission process and timeline

4.2 Internal Progress Reports

All partners will provide an internal progress report on a biannual basis, which is another form of clarifying “quality objectives” as well as “agreed definitions of procedures for acceptance and quality control” and presenting “appropriate tools for planning, monitoring and progress reporting.” The internal progress reports will enable the PC to monitor the progress of the project in relation to work package plans, deliverable submission dates and project milestones as well as to check the resources committed by all partners.

For this reason, a project progress template including a budget table has been developed and will be filled in by all partners.

The progress reports will cover the following project periods:

- R1: M1-M6
- R2: M7-M12
- R3: M13-M18
- R4: M19-M24
- R5: M25-M30
- R6: M31-M36

These internal reports will form the basis of the interim report at M19 and the final report at M36.

4.3 Periodic Reporting

Over the course of the project, two formal periodic reports (each consisting of both technical and financial dimensions) must be submitted to the European Commission, which supplement the reporting and quality standards as laid out above. One is due by the project’s mid-term stage (M19) and one by the concluding stage of the project (M36). These reports will be submitted to the EC for the purpose of reviewing and evaluating the progress of work. The PC is responsible for organising the preparation of both reports.

These reports consist of two parts and should include:

1) Technical report:

- “Part A: contains the structured tables with project information (retrieved from the Grant Management System).

-
- Part B (the narrative part): mirrors the application form and requires the participants to report on differences (delays, work not implemented, new subcontracts, budget overruns etc.) It must be uploaded as PDF document.”⁵⁹

All partners will contribute to the technical reports and particularly all WPLs are responsible for preparing the technical content regarding their WP.

2) Financial report:

- “An explanation of the use of resources and the information on subcontracting and in-kind contributions provided by third parties, from each beneficiary for the reporting period concerned.”⁶⁰
- A Certificate on the Financial Statement (CFS) is needed, if a beneficiary requests an EU contribution of 430 000€ or more from the programme.

In accordance with the criteria of Horizon Europe, it is the responsibility of all partners to complete the financial report for their organisation on the ECAS participant portal. Detailed instructions on the submission process of the periodic financial statement will be circulated to all partners on time.

⁵⁹ European Commission, *Funding and tender opportunities: Periodic Reports* (European Commission, 2022). Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/reports/periodic-reports_en.htm.

⁶⁰ European Commission, *Funding and tender opportunities: Periodic Reports* (European Commission, 2022). Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/reports/periodic-reports_en.htm.

5 Risk Management

The FERMI consortium distinguishes between different types of risks. More specifically, risks are being ranked in consideration of their probability and their impact. The underlying idea is that all risks may carry different weights, depending on whether they are likely to materialise and how grave their ramifications would be. Both types of risks are evaluated along the lines of three different categories: low, medium and high. Accordingly, the overall risk of an impediment to the project can be assigned to one of the categories in the table below. Obviously, a risk is particularly worrisome and requires urgent action in the event that it is very likely to come to force (high probability) and very likely to have serious ramifications (high impact).

Probability	Impact		
	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Medium	Medium

	Low level of risk
	Medium level of risk
	High level of risk

Considering that this deliverable is due at the very early stage of the project (M2), the risks the project is facing have not changed for the time being. Neither have the risk assessments. Accordingly, the overview of the current risks is basically the same as the one given in the GA⁶¹ from which the following risk table has been adapted. Having said that, the FERMI risk table will be regularly reviewed by the consortium during the SC telcos to ensure that any risk that might arise and require proper mitigation measures can be identified and rectified as quickly as possible.

Table 10: Indicative project implementation risks and mitigation measures

Description of Risk	Proposed risk-mitigation measures
<p>Failure to provide comprehensive use exercises and elicit solid requirements. Probability: Low, Impact: High Related to WP2, WP3, WP4</p>	<p>T2.1 will provide the user requirements, while T2.3 will extract the technical/system requirements. All consortium partners will ensure that they provide concrete and comprehensive input in order to bridge any terminology gap and allow a proper elicitation of both requirements.</p>
<p>The limited availability of data (e.g., time and location of the event) on criminal events may have a strong impact on the capacity to analyse and predict offline crimes related to the spread of D&FN. Probability: Low, Impact: Medium</p>	<p>This risk has low probability of occurrence thanks to 1) the high expertise and capabilities of partners involved in the data generation and gathering activities; 2) the presence in the consortium of end users, which already have available data on crime of interest; 3) the use of multiple sources (e.g., official crime statistics, open-source news and press releases). Nonetheless, in the unlikely event of a shortage of data, FERMI will adopt three complementary mitigation measures in the analysis and prediction of offline crimes: 1) Perform additional data collection by automatically extract and analyse additional contents of open-source news. 2) Prioritize AI methodologies that make a 'parsimonious use of data' thus favouring the employment of the most efficient techniques in terms of data usage (for</p>

⁶¹ Grant Agreement, Description of the Action, PART B, p.43-44.

Related to WP3, WP4	example, Machine Learning or Natural Language Processing). 3) Extend the use of alternative approaches (e.g., qualitative assessments) in the identification of relevant security measures related to D&FN and in the understanding of the cultural and societal aspects of the impact of D&FN on offline crimes.
Difficulty and complexity of integrating the constituting technologies in the overall FERMI framework. Probability: Low , Impact: Medium	Project partners have significant expertise in building working system prototypes for their research and development activities. In addition, the project structure of continuous integration and evaluation aims to deal with this issue and reduce the impact of individual problems or delays. Thus, although problems may occur, the project will be able to deliver a working prototype version, even if not all planned features are present.
Insufficient Project Impact / Low Community Building & Stakeholders Engagement. Probability: Low , Impact: Medium Related to WP6	Task 6.2 will build an extended network stakeholder on top of the project consortium partners and will ensure the reach out of a critical mass of stakeholders, policy makers, vendors. Also, dissemination and communication will safeguard significant project impact creation.
Business plan failing to exploit market opportunities. Probability: Medium , Impact: Low Related to WP6	The development of the FERMI business plan will be led by an experienced and professional team under T6.3. Nevertheless, opportunities may be identified by other partners in the domain, or later on in the project, but within its lifecycle. Should this happen, the business plan development leaders will evaluate the opportunities, and try to re-formulate / modify / customise the business plan accordingly in its final iteration to facilitate the exploitation of these opportunities.

In FERMI it has been assessed that there are relatively few risks that are clearly associated with the project and the envisaged output, at least for the time being. However, there are some further external factors and barriers that might impede the project, which are listed here as well, albeit those are not ranked in accordance with the types of risks approach as explained above.

	Barriers	Mitigation measures
Political	<i>(P1) Lack of incentives for governments across the EU to adopt the developed outcomes*. (P2) Data confidentiality, locality and protection - potential restrictions in data usage and sharing across countries. (P3) GDPR regulatory environment changes requiring changes in the design of any data platform*.</i>	FERMI will liaise from the beginning with policy makers, legislation agencies and standardisation bodies to stay at the forefront of updates in the field of trustworthy data management and relevant policies (current and upcoming) in EU. The technologies to be developed will fully conform with GDPR practices to respect data protection and privacy. Two complementary partners (KUL, VUB) bring expertise in this field.
Economic	<i>(E1) New data-driven business models built on shared value generation often lack incentives for users (e.g., LEAs) to share data related to the spread of D&FN. (E2) Uncertainty over regulatory actions might delay investments in the long-term*. (E3) Lack of cooperation from stakeholders (private & public sector, especially from LEAs) might delay in the short-term*.</i>	FERMI will develop a go-to-market strategy throughout the project's execution. A detailed business plan including a market and competitive analysis and operational, financial, marketing, growth and contingency plans will be prepared and appropriately refined over time. To successfully address and overcome the identified barriers to market uptake, FERMI will actively involve relevant stakeholder groups.

Social	<p><i>(S1) Societal resistance against data and information sharing between LEAs, as well as related to the identification of fake news without violating the freedom of speech (S2) Lack of jobs and growth (underinvestment) in related research. (S3) Lack of awareness of the possibilities and benefits of AI-related approaches applied in the finance/banking and health sectors*. (S4) Lack of engagement of stakeholders eliminates the prospect of building a sustainable strategy*.</i></p>	<p>FERMI is investing in raising awareness through a number of initiatives, including among others pursuing synergies with other relevant projects, organising a series of outreach events and informative sessions addressed to the general public and key stakeholders concerning the benefits of its envisioned technological advancements towards the minimization of the risks and effects of D&FN spreading.</p>
Technological	<p><i>(T1) Lack of harmonised certification procedures and standards related to approaches used for the modelling of D&FN spreading (T2) Lack of interoperable solutions (technical standards) and practices (process standards) affecting the actual exploitation of such modelling and risk analysis architectures (T3) Higher user expectations enabled by technology.</i></p>	<p>FERMI will monitor all relevant EU laws and Directives and pursue collaboration and networking with the relevant Agencies to contribute to the harmonisation of test protocols. Collaboration with standardisation bodies will ensure the development process complies with all related standards. Relevant R&I work within and beyond Horizon Europe will feed into the project.</p>

6 Innovation

The goal of this section is to set – at an early stage of the project – the common rules that will drive the exploitation and commercialisation of FERMI’s results, including the management of intellectual property rights (IPR) and the relative competitiveness of the end results. To this end, this section presents the strategic plans for innovation assurance, including technical coordination and management procedures of the technical evolutions within the project, as well as the project progress in terms of achieved innovation. A set of mechanisms are put in place, which will be coordinated within the DKMC – ensuring that throughout the project a strong link is maintained between concept, final solution and end-user needs & goals.

6.1 Technical and Innovation strategy plan

6.1.1 Technical management approach

In an attempt to streamline the management of all technical activities towards defining and realising the functional value of the FERMI platform and individual components, the consortium has agreed to follow the project’s technical development activities under the premises of the aforementioned WPs. Each technical WP leader is responsible for overseeing all related activities and coordinating with the FERMI Technical Manager (ITML).

Each technical WP will meet on a regular basis (i.e. weekly, bi-weekly) and will use a dedicated Git project for tracking items. In parallel with the regular WP meetings, the Technical Manager will coordinate on a monthly basis a 1.5h DKMC meeting to present regular technical and innovation updates, next steps and discuss issues and other concerns with regard to the technical implementation. It should be noted that in these meetings all partners are welcome to participate, and this provides a good opportunity for all partners to be up to date with regard to the technical developments and the status of both individual components and the integrated platform.

Furthermore, guidelines for intellectual property creation and a licensing/filing strategy to protect the IP generated through FERMI will be introduced and distributed to the consortium in order to ensure a consistent and transparent publication process of the FERMI results supported by the innovation management approach that is introduced in the following section.

6.1.2 Innovation management approach

Among a variety of Innovation Management strategies, the approach chosen for the FERMI project is commonly known as Open Innovation.⁶² This approach supports the idea that innovation occurs because of interactions between different actors, rather than being the result of an isolated genius.⁶³ This innovation concept is supported by the European Commission and its Horizon 2020 program and is the basis of the FERMI project.⁶⁴

⁶² Felina, Teppo, and Todd R. Zenger, ‘Closed or open innovation? Problem solving and the governance choice’, *Research Policy*, 43 (2014), 914-925.

⁶³ Von Hippel, E.A., *The sources of innovation* (New York NY: Oxford University Press, 1998).

⁶⁴ European Commission, *Open Innovation. Open Science. Open to the world. A vision for Europe* (Brussels: Directorate-General for Research and Innovation, Directorate A – Policy Development and Coordination, Unit A1 – Internal and external communication, 2016). Available at: <https://digital-strategy.ec.europa.eu/en/library/open-innovation-open-science-open-world>.

Open Innovation is a strategy to leverage internal and external sources of ideas and take them to the market through multiple paths. Towards this direction, collaboration is the key to achieve high innovation rates and efficient product development. The cooperation capacity of organisations through agreements allows ideas to flow across organisational boundaries.⁶⁵ The concept of Open Innovation is opposed to that of Closed Innovation,⁶⁶ where the overall innovation process – from ideas to marketing – happens within the organisation and profit is generated by pioneering innovation in the current market. In the Open Innovation model, both the internal and the external organisational environments are involved in the process.

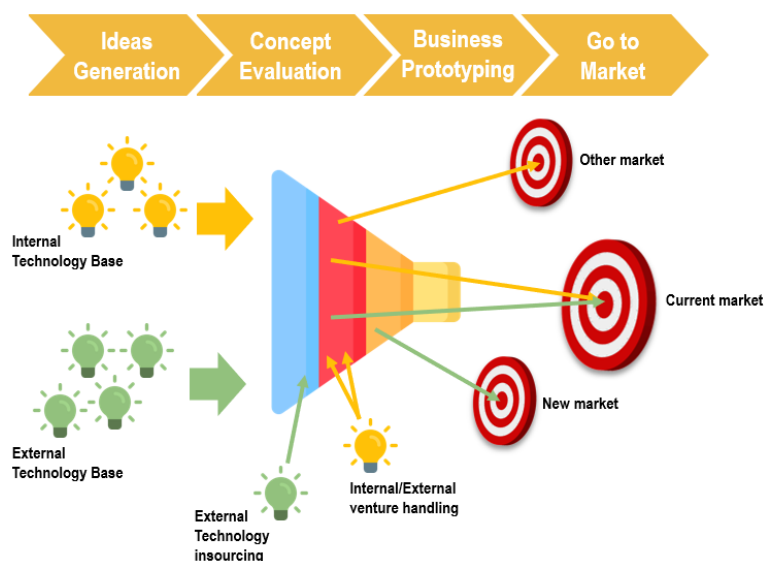


Figure 5: Open Innovation Model

Amongst the advantages in developing Open Innovation strategies are the possibility of exploring new markets and the increased flexibility. Furthermore, these strategies facilitate access to those new markets and new knowledge, allow to share both risks and resources in the process, support innovation, and foster the creation of new value, the confrontation of ideas and practices, as well as the creation of synergies.

When following an Open Innovation strategy, particular attention will be paid to overcoming critical issues, such as the dependence on the underlying value system, the identification of the “added value” that is contributed by each partner, the distribution of income and liabilities, and the change in valuable aspects from tangible to intangible.

In the development of an Open Innovation model, several processes can be followed:

- **Outside-in process:** organisations invest in cooperation with other agents and integrate external knowledge. They must rely on their absorption capacity to integrate sophisticated and costly technology. They also must recognise the value of new external information, assimilate that information, and apply it to the market, taking advantage of efficient generation and integration processes.
- **Inside-out process:** to outsource internal knowledge and technology. This allows organisations to reduce fixed costs of the R&D activities, to set them as a reference in the market and their products

⁶⁵ Chesbrough H., *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Boston, MA: Harvard Business School Press, 2003).

⁶⁶ Chesbrough, H. and Wim Vanhaverbeke, Joel West (eds), *Open Innovation: Researching a New Paradigm* (Oxford: Oxford University Press, 2006).

and/or services as a standard, and to provide benefits from licenses and patents. Organisations must rely on their multiplicative capacity to transfer internal knowledge to their parties. They must select the most appropriate partners and must be able to code and share their knowledge.

- **Coupled process:** cooperation with other participants through strategic networks for an extended period. Greater benefits can be obtained, and success depends on the choice of the right partners, as well as on the integration of the external knowledge and skills.⁶⁷ In this process, organisations need to develop an effective connection capacity to build and maintain relationships with partners, particularly with complementary entities and competitors.

Table 11 summarises the main Open Innovation Activities for each process:

Table 11: Open Innovation activities

Inside-Out	Outside-In	Coupled
Licensing out	Licensing in	Co-development
Corporate venture capitalist	Merger & Acquisition	Collaboration
Staff Exchange	Innovation contests	Co-marketing
	Acquisition of right	Commercialisation
	Outsourcing R&D	Co-promotion
	Technology scouting	Cross-distribution

Within the Open Innovation model, the **Coupled process** naturally fits with the characteristics and the multiple purposes of a collaborative experience, like FERMI.

6.1.3 Monitoring and coordination

FERMI will set up a process to monitor and coordinate the technical and innovation progress of the demonstrators. This process will be built around the project’s objectives. To this respect, as part of the first semester work, the monitoring process will focus on the identification of the innovation elements (Key Innovation Results - KIR), aiming to provide technical support on the design of their implementation, technical risk assessment, and mitigation and contingency actions for involved partners. Moreover, it will also target the project’s Key Exploitable Results (KER), aiming to facilitate the identification of market needs, link those needs to the value proposition of the KIR and recognise potential business models that will allow for the successful deployment and exploitation of the KIR.

The monitoring of the technical and innovation progress of FERMI’s integrated solution includes not only the purely technical evolution but also the related novelties. An essential part of the technical and innovation management activities is to monitor the continuously evolving market needs to adjust the implementation of FERMI solutions to better address those needs and challenges. Therefore, the Technical Manager, ITML, and the DKMC will ensure that the following information will be collected:

- **The technical progress** of implementing the FERMI integrated solution and individual components.
- **The progress on the innovation side** of the integrated solution and individual components (and respective KIRs). This progress includes information on innovation and novel ideas that have or will

⁶⁷ Gassmann, O. and Ellen Enkel, *Towards a Theory of Open Innovation: Three Core Process Archetypes* (R&D Management Conference (RADMA), 2004).

be achieved during FERMI towards Technology Readiness Level (TRL) and Market Readiness Level (MRL) advancements of the technologies.

- **The market needs, changes and challenges** that may influence the technologies' implementation, innovation and market value during FERMI, as well as the overall project's objectives.
- **Novel business models** that will arise through the implementation of innovations.

The Technical Manager and the technical partners will use the following tools to facilitate the data collection and the monitoring process:

- **KR/KPI Evaluation Matrix:** As part of quantifying innovation through innovation metrics, the consortium will develop and use an Evaluation Matrix to keep track of the number of metrics (technology-, business-, demonstration-, impact-related) which will be based on those already defined in the GA's Part B in the form of Key Results (KRs) / Key Performance Indicators (KPIs). The matrix will be available in FERMI's online collaborative tool and will be regularly updated by all KIR owners and discussed during the regular WP meetings. The file will state the evaluation strategy, link with any deliverable for evaluation progress, current status and latest review.
- **Technical and Innovation progress questionnaire:** The FERMI partners will use the questionnaire to provide information on the KIRs and developed solutions based on a planning-developing-implementation-monitoring approach. The questionnaire will be prepared by the Technical Manager in collaboration with the leader of T6.4 Market Analysis and Business Modelling towards project's exploitation (INTRA) (to minimise the distribution of separate questionnaires that would have significant overlap) with the aim of facilitating the monitoring process and creating a homogeneous data collection system. Each partner responsible for each KIR, fills in the questionnaire, which is then consolidated by the Technical Manager. The data collected will be used to monitor the technical and innovation progress at standard time intervals.

6.1.4 General plan and tool description

The implementation of the coupled process within FERMI (see above) will be based on a four-phases plan that will serve the process and will use as input the findings of the project. These phases are: **mapping, scouting, assessment,** and **exploitation,** and are depicted in the following figure (Figure 6).

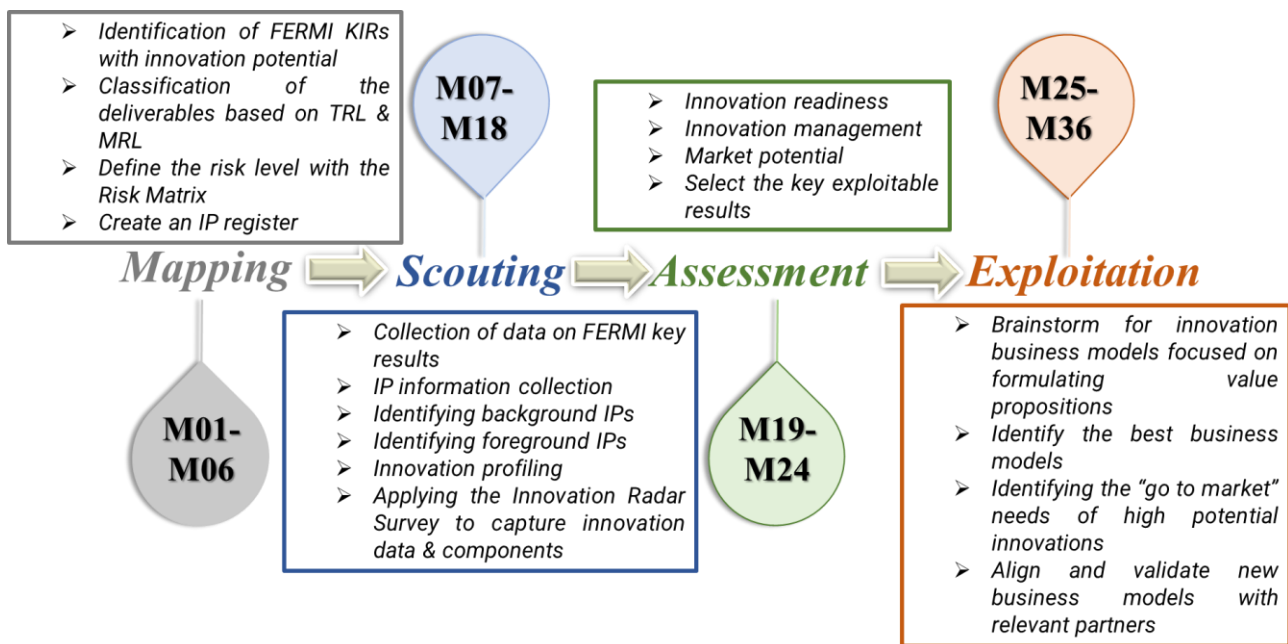


Figure 6: Innovation time-plan

In order to identify, classify and organise the FERMI deliverable from an innovation standpoint the first step is the **mapping phase**. The Technical Manager will lead this process in cooperation with the Project Coordinator. The classification of the FERMI deliverables in terms of their innovation potential will take place following the TRL and MRL criteria. The innovation risk for each deliverable has been evaluated through a risk matrix. The mapping process allows us to create an innovation roadmap for FERMI, adopting the Stage Gate Model (SGM) approach, which is an industry-validated protocol to monitor the Innovation evolution of the project.

The following step is the **scouting process**, a rolling activity driven by an innovation roadmap and led by the Technical Manager in cooperation with the WP leaders and the Project Coordinator. The Technical Manager collects the project results, focusing on IP during the project execution. According to the innovation roadmap, WP leaders, in collaboration with the KIR owners, will analyse every result, selecting the ones with high innovation potential. The selection and analysis of the innovation potential of results/actions will be done by using the Innovation Radar Survey method⁶⁸ and its questionnaire, which will allow the Technical Manager to draw an innovation assessment in agreement also with the EU evaluation rules. The assessment process will be performed by a set of indicators, namely the Innovation Readiness Indicator, Innovation Management Indicator, and Market Potential Indicator and then evaluating the Innovation Potential Indicator conceived to measure the Real-Win-Worth It (R-W-W) screening criteria⁶⁹ for the business impact of the innovation. The assessment process is the basis for the exploitation phase, during which the Technical Manager, the Project Coordinator and the exploitation experts will analyse and select the business model that can maximise the impact of the innovation among the market segments.

⁶⁸ European Commission, *Innovation Radar: Shaping Europe's digital future* (European Commission, 2022). Available at: <https://ec.europa.eu/digital-single-market/en/innovation-radar>

⁶⁹ Day, G., 'Is It Real? Can We Win? Is It Worth Doing? Managing Risk and Reward in an Innovation', *Harvard Business Review* (2007). Available at: <https://hbr.org/2007/12/is-it-real-can-we-win-is-it-worth-doing-managing-risk-and-reward-in-an-innovation-portfolio>.

6.1.4.1 Innovation Phases

Each phase presented in the general plan above is a structured set of activities, with clearly defined responsibilities. These activities have specific objectives, starting inputs, involved actors and final outputs. For each process, we define the items as follows:

- **Objective:** scope of the activity
- **Inputs:** inputs to the activity and the persons who provide them
- **Actors:** responsibility assignment matrix (responsible, accountable, consulted, and informed – RACI) to identify the roles in completing the process activities:
 - Responsible: main executor of the process
 - Accountable: the person who is accountable for the correct and thorough completion of the process
 - Consulted: the people who provide information for the process
 - Informed: the people kept informed of progress of the process.
- **Activities:** list of the activities
- **Outputs:** description of outputs of a particular activity

A description of the implementation of each phase to the specific needs and characteristics of FERMI is presented in the following sub-sections.

6.1.4.1.1 Mapping

Organise the FERMI outcomes identifying the ones with innovation potential, collecting the IP background statement and creating an innovation framework.

Objective	Mapping FERMI KIRs with innovation potential			
Input	FERMI project outputs/findings			
Actors	Responsible	Accountable	Consulted	Informed
	Technical Manager	Project Coordinator	All partners	All partners
Actions	<ul style="list-style-type: none"> – Identification of FERMI KIRs with innovation potential – Classification of the deliverables using the following criteria <ul style="list-style-type: none"> • TRL – Technology Readiness Level • MRL – Market Readiness Level – Define the innovation path framework using the SGM approach – Define the risk level with the Risk Matrix – Create an IP register 			
Outputs	Innovation framework List of Key Innovation Results IP Register			

6.1.4.1.2 Scouting

Following the innovation framework, the WP Leaders, coordinated by the Technical Manager and the Project Coordinator, collect all the innovation-relevant information using the European Union Innovation Radar Questionnaire during the project execution. During the innovation profile action, the Technical Manager collects and organises the information about the results with innovation potential. At this stage the results are called innovation candidates and are ready to be evaluated by the Technical Manager during the assessment phase.

Objective	Capturing information and innovation profiling related to FERMI results			
Input	FERMI KIRs			
Actors	Responsible	Accountable	Consulted	Informed
	Project Coordinator	Technical Manager	All partners	All partners
Actions	<ul style="list-style-type: none"> – Collection of data and information on FERMI project’ key results – IP information collection <ul style="list-style-type: none"> • Identifying background IPs • Identifying foreground IPs – Innovation profiling <ul style="list-style-type: none"> • Applying the Innovation Radar Survey to capture innovation data/components and information 			
Outputs	List of innovation candidates Updated IP Register			

A template document with the Innovation Radar Questionnaire (16 questions) will be prepared and will be shared among all partners during the scouting phase. The document will also include the evaluation score (from 1 to 10) to each question of the survey. This will provide a quantitative starting evaluation of the proposed “candidates”. A six-month schedule will be drawn by the Technical Manager for collecting, updating and analysing the innovation questionnaires that will be discussed in the assessment phase (see below).

6.1.4.1.3 Assessment

The list of innovation candidates will be evaluated and ranked by the Technical Manager and the Project Coordinator following the EU Innovation Radar guidelines. The innovation candidates with a high rank of innovation potential will be qualified as KERs and moved to the next level, the Exploitation Phase. These results will provide the foundation of this endeavour and will be jointly assessed together with the innovation candidates during this phase.

Objective	Analyse and rank the FERMI innovations to select the key exploitable results			
Input	List of potential innovation results and framework			
Actors	Responsible	Accountable	Consulted	Informed
	Technical Manager	All partners	Project Coordinator	WP leaders

Actions	<p>Assessment analysis and focus sessions to rank and evaluate the framework to rank innovation potential from the standpoints as follows:</p> <ul style="list-style-type: none"> – Innovation readiness – Innovation management – Market potential – Select the key exploitable results
Outputs	List of KERs

6.1.4.1.4 Exploitation

The Technical Manager supported by the T6.4 leader will analyse each key exploitable result to identify the best business model that can be adopted to maximise the business growth of the results. As a result of this activity, a canvas model will be developed for each KER. This activity will be directly connected with the business plan activity.

Objective	Identify the business model for developing the business plan			
Input	List of KERs			
Actors	Responsible	Accountable	Consulted	Informed
	Technical Manager	All partners	Project Coordinator & T6.4 leader	WP leaders
Actions	<ul style="list-style-type: none"> – Brainstorm for innovation business models focused on formulating value propositions – Identify the best business models which can exploit the innovation result – Identifying the “go to market” needs of high potential innovations – Align and validate new business models with industrial relevant partners 			
Outputs	Business model definition			

6.2 Intellectual Property Rights (IPR) Management

As clarified above, T1.2, which concerns the technical management, includes the commitment to “introduce and distribute guidelines for intellectual property creation, to ensure a consistent and transparent publication process of FERMI results towards innovation management.”⁷⁰

Accordingly, this subsection is to provide the FERMI consortium with some basic guidelines as to how to avoid potential pitfalls and issues relating to IPR that the partners may encounter during the lifetime of the project. Having said that, it appears there is no need to go into too much detail, considering that the IPR issue has already been addressed in great depth in the Grant Agreement and the Consortium Agreement (CA). It should be clarified that this set of remarks is to be considered in conjunction with those two agreements signed by all Beneficiaries. The purpose is to summarise and share key information on some focal points of the subject matter such as (joint) ownership, transfer of results, access rights and dissemination proceedings, which are

⁷⁰ Grant Agreement, Description of the Action, PART A, p.6.

derived from both agreements. However, in case of doubt, the Grant Agreement as well as the CA take precedence over the subsequent remarks.

6.2.1 (Joint) Ownership

When it comes to ownership, it is stipulated in both the Grant Agreement and the CA that results are owned by the beneficiaries that generate them.⁷¹

Having said that, both agreements clarify that joint ownership of results is possible too if “two or more beneficiaries [...]

- [...] have jointly generated them and
- it is not possible to:
 - establish the respective contribution of each beneficiary, or
 - separate them for the purpose of applying for, obtaining or maintaining their protection.

The joint owners must agree — in writing — on the allocation and terms of exercise of their joint ownership (‘joint ownership agreement’) [...].⁷²

Besides these guidelines and building on the further rules as enshrined in the Grant Agreement, the FERMI consortium has taken additional steps “(i) to ensure that there is common understanding about who are the joint owners of every joint Result and (ii) in order to agree the level of intellectual contribution of each of the joint owners from an early stage of its implementation.”⁷³ More specifically, it has been agreed that

- a) “any Party contributing to an activity resulting in jointly owned Results, must inform the other potential joint owners and try to reach the corresponding acceptance of the proposed joint ownership.
- b) This notification shall be done at least to be processed by the next General Assembly meeting [for an overview of the role and responsibilities of the General Assembly, see Section 2.1.7] convened following the start of the joint ownership.”

Any conflict raised in the joint ownership (including retrospective claims on joint-ownership contributions), will be escalated to the General Assembly for final decision, or [...] [in accordance with conflict resolution mechanisms] when the conflict cannot be solved amicably.

Unless otherwise agreed:

- each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research and teaching activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s).
- each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and to grant non-exclusive licenses to third parties (without any right to sub-license), if the other joint owners are given: (a) at least 45 calendar days advance notice; and (b) Fair and Reasonable Conditions, whether financial or not.

The joint owners shall agree in writing on the allocation of ownership and terms of exercising, protecting, disseminating as well as on all protection measures and the division of related costs in advance of any such protection measures being undertaken by any of the joint owners. The joint owners shall enter into good faith

⁷¹ Grant Agreement, ANNEX 5, p.4.; Consortium Agreement, p.17.

⁷² Grant Agreement, ANNEX 5, p.4.

⁷³ Consortium Agreement, p.17.

discussions in order to agree on an appropriate course of action for filing application(s) for Intellectual Property Rights in such joint Result, including the decision as to which Party is to be entrusted with the preparation, filing and prosecution of such application(s) and in which countries of the world such application(s) for Intellectual Property Rights are to be filed. Unless the concerned Parties agree otherwise on a case by case basis, or explicitly provided otherwise herein, all costs related to application(s) for Intellectual Property Rights in joint Results and Intellectual Property Rights resulting from such application(s) shall be shared proportionally between the joint owners.”⁷⁴

6.2.2 Transfer of results

The Grant Agreement stipulates that ownership of results may be transferred by the relevant consortium partners “provided this does not affect compliance with their obligations under the Agreement.”⁷⁵ In this case, they “must ensure that their obligations under the Agreement regarding their results are passed on to the new owner and that this new owner has the obligation to pass them on in any subsequent transfer. Moreover, they must inform the other beneficiaries with access rights of the transfer at least 45 days in advance (or less if agreed in writing) unless agreed otherwise in writing for specifically identified third parties including affiliated entities or unless impossible under the applicable law.”⁷⁶

The consortium has agreed that “[e]ach Party may identify specific third parties it intends to transfer the ownership of its Results to” and that “[t]he other Parties [...] waive their right to prior notice and their right to object to such a transfer [...]” Having said that, “[t]he transferring Party shall, however, at the time of the transfer, inform the other Parties of such transfer and shall ensure that the rights of the other Parties under the Consortium Agreement and the Grant Agreement will not be affected by such transfer.”

Moreover, the FERMI consortium “recognize[s] that in the framework of a merger or an acquisition of an important part of its assets, it may be impossible under applicable EU and national laws on mergers and acquisitions for a Party to give at least 45 calendar days prior notice for the transfer as foreseen in the Grant Agreement.” The consortium has also clarified that “[t]he obligations above apply only for as long as other Parties still have – or still may request – Access Rights to the Results.”⁷⁷

6.2.3 Access rights

The access rights issue is clearly addressed by the Grant Agreement’s Article 16.1. More specifically, it is laid out that “[t]he beneficiaries must give each other and the other participants access to the background identified as needed for implementing the action.”⁷⁸ There are further rules and some exceptions (concerning how to “[e]xercise of access rights — Waiving of access rights — No sub-licensing,” “[a]ccess rights for implementing the action,” “[a]ccess rights for exploiting the results,” “[a]ccess rights for entities under the same control,” “[a]ccess rights for the granting authority, EU institutions, bodies, offices or agencies and national authorities to results for policy purposes — Horizon Europe actions,” “[a]ccess rights for the granting authority, Euratom institutions, funding bodies or the Joint Undertaking Fusion for Energy — Euratom

⁷⁴ Consortium Agreement, p.17-18.

⁷⁵ Grant Agreement, ANNEX 5, p.6.

⁷⁶ Grant Agreement, ANNEX 5, p.6.

⁷⁷ Consortium Agreement, p.18-19.

⁷⁸ Article 16.1 specifies the term “Background”, which “means any data, know-how or information — whatever its form or nature (tangible or intangible), *including any rights such as intellectual property rights* [emphasis added] — that is: (a) held by the beneficiaries before they acceded to the Agreement and (b) needed to implement the action or exploit the results. If background is subject to rights of a third party, the beneficiary concerned must ensure that it is able to comply with its obligations under the Agreement.” (See Grant Agreement, General, p.33-34).

actions” and “[a]dditional access rights”), though, which are described in Annex 5. Considering how specific these rules are, it would be beyond the scope of this sub-section to address them in greater detail.

However, it should be clarified that the consortium partners have inserted in the FERMI CA a list of Background that is excluded from obligations to grant access rights. In other words, they “have identified and agreed on the Background for the Project and have also, where relevant, informed each other that Access to specific Background is subject to legal restrictions or limits.” Moreover, all partners have agreed on a set of general principles governing access rights, which are listed as follows.

- “Each Party shall implement its tasks in accordance with the Consortium Plan and shall bear sole responsibility for ensuring that its acts within the Project do not knowingly infringe third party property rights.”
- “Any Access Rights granted exclude any rights to sublicense unless expressly stated otherwise.”
- “Access Rights shall be free of any administrative transfer costs.”
- “Access Rights are granted on a non-exclusive basis.”
- “Results and Background shall be used only for the purposes for which Access Rights to it have been granted.”
- “All requests for Access Rights shall be made in writing. The granting of Access Rights may be made conditional on the acceptance of specific conditions aimed at ensuring that these rights will be used only for the intended purpose and that appropriate confidentiality obligations are in place.”
- “The requesting Party must show that the Access Rights are Needed.”⁷⁹

6.2.4 Dissemination and Reporting

Dissemination can be seen as the means (i.e., press releases, conferences, scientific publications, exhibitions, workshops, newsletters, websites, etc.) through which research results are presented to the public. It is important to notice that official publications in the course of a protection right application (e.g., the compulsory publication of a patent application after its filing) are not considered dissemination. The target group of dissemination may be the general public or a specific group of professionals in a determined sector. An overview on the most successful means of dissemination, as well as useful suggestions on how to arrange an effective communication strategy, can be found on the European Commission’s European Research Executive Agency’s website.⁸⁰

Any dissemination activity shall be reported within the framework of WP 6, including sufficient details/references. The FERMI Dissemination Manager (LC) also keeps a database template in the collaboration tool (OwnCloud), which is regularly updated by all FERMI partners with regard to dissemination activities (fulfilled and upcoming). All publications also need to acknowledge EU funding (in the form of stating that the relevant output has been “[f]unded by the European Union”).⁸¹

The FERMI Beneficiaries are expected to regularly update the list of publications in due course (including their publication plans) so any IPR issues can be raised as soon as possible.

Moreover, each Beneficiary has to upload the accepted publication (released version) in a dedicated folder and to inform the PC that the publication is available to be sent to the Commission.

⁷⁹ Consortium Agreement, p.20-21.

⁸⁰ European Commission, European Research Executive Agency: *Horizon Europe – Dissemination and exploitation* (European Commission, 2022). Available at: https://rea.ec.europa.eu/horizon-europe-dissemination-and-exploitation_en.

⁸¹ European Commission, European Research Executive Agency: *Communicating about your EU-funded project* (European Commission, 2022). Available at: https://rea.ec.europa.eu/communicating-about-your-eu-funded-project_en.

7 Conclusion

This deliverable gives an overview of the essential management structures of the FERMI project. More specifically, it assigns the key roles to certain partners to divide the workload and ensure that the most fundamental obligations are fully met and properly monitored by experienced partners that are well-qualified to take the lead on the to-be-addressed matter. The set-up of the project's boards and committees is described as well and so is the assignment of WP and deliverable leads as well as key milestones. The FERMI Project Management Playbook proceeds with an overview of the communication efforts concerning in-person meetings, the content management system, the communication tools and the project's visual identity and concludes with a detailed explanation of the reporting, monitoring and quality assurance proceedings, the project's risk management and its innovation management approach (including the IPR notion).

References

- [1] Chesbrough H., *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Boston, MA: Harvard Business School Press, 2003).
- [2] Chesbrough, H. and Wim Vanhaverbeke, Joel West (eds), *Open Innovation: Researching a New Paradigm* (Oxford: Oxford University Press, 2006).
- [3] Consortium Agreement.
- [4] Day, G., ‘Is It Real? Can We Win? Is It Worth Doing? Managing Risk and Reward in an Innovation’, *Harvard Business Review* (2007). Available at: <https://hbr.org/2007/12/is-it-real-can-we-win-is-it-worth-doing-managing-risk-and-reward-in-an-innovation-portfolio>.
- [5] European Commission, *EU Grants: How to handle security-sensitive projects. Projects with sensitive and classified information* (Brussels: European Commission, 2021).
- [6] European Commission, *Funding and tender opportunities: Periodic Reports* (European Commission, 2022). Available at: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/reports/periodic-reports_en.htm.
- [7] European Commission, *Innovation Radar: Shaping Europe’s digital future* (European Commission, 2022). Available at: <https://ec.europa.eu/digital-single-market/en/innovation-radar>
- [8] European Commission, *Open Innovation. Open Science. Open to the world. A vision for Europe* (Brussels: Directorate-General for Research and Innovation, Directorate A – Policy Development and Coordination, Unit A1 – Internal and external communication, 2016). Available at: <https://digital-strategy.ec.europa.eu/en/library/open-innovation-open-science-open-world>.
- [9] The European Commission, *PROGRAMME SECURITY INSTRUCTION CONCERNING Horizon Europe Programme (SHORT TITLE: HORIZON EUROPE PSI)* (Brussels: European Commission, 2020).
- [10] European Commission, European Research Executive Agency: *Communicating about your EU-funded project* (European Commission, 2022). Available at: https://rea.ec.europa.eu/communicating-about-your-eu-funded-project_en.
- [11] European Commission, European Research Executive Agency: *Horizon Europe – Dissemination and exploitation* (European Commission, 2022). Available at: https://rea.ec.europa.eu/horizon-europe-dissemination-and-exploitation_en.
- [12] Felina, Teppo, and Todd R. Zenger, ‘Closed or open innovation? Problem solving and the governance choice’, *Research Policy*, 43 (2014), 914-925.
- [13] Gassmann, O. and Ellen Enkel, *Towards a Theory of Open Innovation: Three Core Process Archetypes* (R&D Management Conference (RADMA), 2004).
- [14] Grant Agreement.
- [15] Landesamt für Digitalisierung, Breitband und Vermessung, *IT-Dienstleistungszentrum des Freistaats Bayern, Datenaustausch mit Externen* (Landesamt für Digitalisierung, Breitband und Vermessung, 2022). Available at: http://www.it-dlz.bybn.de/dienstleistungen/datenaustausch_owncloud/index.html.
- [16] Von Hippel, E.A., *The sources of innovation* (New York NY: Oxford University Press, 1998).

Annex A Fermi Deliverable Tracker

Lead beneficiaries are kindly asked to share a ToC with INTRA (Quality Manager), BPA (Coordinator) and the key contributors 2,5 months prior to the deliverable's final submission date.

Lead beneficiaries are kindly asked to share their drafts with the peer, EAB and SAB reviewers, as listed below (with INTRA and BPA in cc).

Reviewers are kindly asked to get back to the lead beneficiaries in one week's time (with INTRA and BPA in cc).

Lead beneficiaries are kindly asked to share a revised draft with INTRA and BPA 15 days prior to the final submission date.

Deliverable	Title	Lead Beneficiary	Dissemination Level	Draft Submission to Peer Reviewers	Draft Submission to EAB Reviewer	Draft Submission to SAB Reviewer	Final Submission Date
D1.1	Overall Progress & QA Management, Innovation Management and Ethics Management Report	BPA	SEN	31 August 2023 M11 ITML/IANUS	31 August 2023 M11 Flavia Giglio	31 August 2023 M11 Paraskevas Bourgos	30 September 2023 M12
D1.2	Overall Progress & QA Management, Innovation Management and Ethics Management Report	BPA	SEN	31 August 2024 M23 SPA/LC	31 August 2024 M23 Dimitra Markopoulou	31 August 2024 M23 Paraskevas Bourgos	30 September 2024 M24
D1.3	Overall Progress & QA Management, Innovation Management and Ethics Management Report	BPA	SEN	31 August 2025 M35 BFP/IANUS	31 August 2025 M35 Vagelis Papakonstantino	31 August 2025 M35 Paraskevas Bourgos	30 September 2025 M36
D1.4	FERMI Data Management Plan	VUB	SEN	28 February 2023 M5 ITML/BIGS	28 February 2023 M5 Sven-Eric Fikenscher	28 February 2023 M5 Tobias Mattes	31 March 2023 M6

D1.5	FERMI Project Management Playbook	BPA	PU	01 November 2022 M2 PUCF/INTRA	01 November 2022 M2 Dimitra Markopoulou	01 November 2022 M2 Léonie Bouwknegt	30 November 2022 M2
D2.1	FERMI starting point package	INTRA	PU	28 February 2023 M5 ITML/SPA	28 February 2023 M5 Vagelis Papakonstantinou	28 February 2023 M5 Tobias Mattes	31 March 2023 M6
D3.1	Fermi technology facilitators package 1st Version	UCSC	PU	31 December 2023 M15 INTRA/FMI	31 December 2023 M15 Flavia Giglio	31 December 2023 M15 Tobias Mattes	31 January 2024 M16
D3.2	Fermi technology facilitators package	UCSC	PU	28 February 2025 M29 ATOS/FMI	28 February 2025 M29 Flavia Giglio	28 February 2025 M29 Paraskevas Bourgos	31 March 2025 M30
D3.3	FERMI behaviour analyses and community resilience facilitators package 1 st Version	BIGS	PU	31 December 2023 M15 BPA/CONV	31 December 2023 M15 Dimitra Markopoulou	31 December 2023 M15 Léonie Bouwknegt	31 January 2024 M16
D3.4	FERMI behaviour analyses and community resilience facilitators package	BIGS	PU	28 February 2025 M29 INOV/BPA	28 February 2025 M29 Vagelis Papakonstantinou	28 February 2025 M29 Léonie Bouwknegt	31 March 2025 M30
D4.1	The FERMI integrated solution 1st version	INTRA	SEN	28 February 2024 M17 BPA/PUCF	28 February 2024 M17 Dimitra Markopoulou	28 February 2024 M17 Mariana A. Risetto	31 March 2024 M18

D4.2	The FERMI integrated solution	INTRA	SEN	28 February 2025 M29 ATOS/IANUS	28 February 2025 M29 Vagelis Papakonstantinou	28 February 2025 M29 Mariana A. Risetto	31 March 2025 M30
D4.3	The FERMI disinformation watch 1st version	INOV	SEN	28 February 2024 M17 UCSC/LC	28 February 2024 M17 Flavia Giglio	28 February 2024 M17 Pirjo Jukarainen	31 March 2024 M18
D4.4	The FERMI disinformation watch	INOV	SEN	28 February 2025 M29 BIGS/CONV	28 February 2025 M29 Flavia Giglio	28 February 2025 M29 Pirjo Jukarainen	31 March 2025 M30
D5.1	FERMI 1st execution report	SPA	SEN	28 February 2024 M17 ATOS/ITML	28 February 2024 M17 Dimitra Markopoulou	28 February 2024 M17 Tobias Mattes	31 March 2024 M18
D5.2	FERMI 1st execution reports	SPA	SEN	30 June 2024 M21 INTRA/BIGS	30 June 2024 M21 Vagelis Papakonstantinou	30 June 2024 M21 Tobias Mattes	31 July 2024 M22
D5.3	The FERMI final execution reports & assessments	IANUS	SEN	31 August 2025 M35 BIGS/UCSC	31 August 2025 M35 Sven-Eric Fikenscher	31 August 2025 M35 Paraskevas Bourgos	30 September 2025 M36
D5.4	The FERMI Training curricula for officers & sessions' execution report	PUCF	SEN	31 August 2025 M35 BPA/INOV	31 August 2025 M35 Flavia Giglio	31 August 2025 M35 Léonie Bouwknecht	30 September 2025 M36

D6.1	The FERMI outreach management facilitators package	LC	PU	31 December 2022 M3 ITML/INTRA	31 December 2022 M3 Sven-Eric Fikenscher	31 December 2022 M3 Pirjo Jukarainen	31 January 2023 M4
D6.2	FERMI outreach and collaboration management report 1 st Version	LC	PU	28 February 2024 M17 BIGS/UCSC	28 February 2024 M17 Sven-Eric Fikenscher	28 February 2024 M17 Vassilios Chatziannakis	31 March 2024 M18
D6.3	FERMI outreach and collaboration management report	LC	PU	31 August 2025 M35 CONV/IANUS	31 August 2025 M35 Sven-Eric Fikenscher	31 August 2025 M35 Vassilios Chatziannakis	30 September 2025 M36
D6.4	FERMI Market analyses and business modelling towards exploitation	INTRA	PU	31 August 2025 M35 ATOS/ITML	31 August 2025 M35 Sven-Eric Fikenscher	31 August 2025 M35 Pirjo Jukarainen	30 September 2025 M36
D7.1	H - Requirement No. 1	BPA	SEN	30 November 2022 M2 KU Leuven/VUB	30 November 2022 M2 Dimitra Markopoulou	30 November 2022 M2 Mariana A. Risetto	31 December 2022 M3
D7.2	POPD - Requirement No. 2	BPA	SEN	30 November 2022 M2 KU Leuven/VUB	30 November 2022 M2 Flavia Giglio	30 November 2022 M2 Mariana A. Risetto	31 December 2022 M3
D7.3	AI - Requirement No. 3	BPA	SEN	31 May 2023 M8 KU Leuven/VUB	31 May 2023 M8 Vagelis Papakonstantinou	31 May 2023 M8 Mariana A. Risetto	30 June 2023 M9

Annex B Review Template

Deliverable Number									
Deliverable Name									
Version									
Review or Response by author	Review result ● 1								
	<table border="1"> <tr> <th>Organisation</th> <th>Name</th> <th>Email</th> <th>Phone</th> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Organisation	Name	Email	Phone				
Organisation	Name	Email	Phone						
Deliverable Author									
Reviewer									

Key

Needs substantial rework or additional work
Is of reasonable quality, needs some re-work
OK, perhaps some minor comments

Content

#	Criteria	Explanation	Risk level	Comments	Suggested mitigation	Implemented ?
1.1	Main objective of the deliverable	Does it set out to do what it says in DoW?				
1.2	References and building on previous work	Have they overlooked any state of the art, previous work, related projects, regulations or best practices?				
1.3	Methodology	Is work, development, trial, experiment or study being conducted in a sensible way?				
1.4	Conformance of Results	Is the deliverable on track to do what was promised?				
1.5	Usefulness of results	Is the deliverable (and associated results) actually useful to downstream tasks or customers? Is it clear that the results are useful and relevant? Is it clear how the results can be accessed? Are plans realistic and actionable? Is it clear that they are not committing downstream tasks to something impossible? For example KPI targets which cannot be reached or measured.				
Structure						
2.1	Consistency with Description of work	Can the reader easily tell (e.g. by looking at the table of contents) where in the document each point in the DoW is addressed? Is it clear that the deliverable reflects the description of work?				
2.2	Structure	Is structure of the deliverable logical and easy to follow? If you feel it is not, please suggest changes to the structure to make it more accessible.				

Overall conclusion

#	Criteria	Explanation	Score	Explanation of Score by Reviewer	Suggested improvements	Response from Author/Writer
3.1	Risk to Quality	Green - on track Amber - some adjustment required Red - serious risks to deliverable quality	● 1			
Any other remarks						