DG DIGIT B3
Reusable Solutions

EU-FOSSA 2 Project Charter

Preparatory action — Governance and quality of software code - Auditing of free and open source software (26 03 77 06)

Date: 04/05/2018
Doc. Version: 1.7
Template Version: 2.5

This template is based on PM² V2.5

For the latest version of this template please visit the PM² Wiki

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 3

2 CONSIDERATIONS ON THE BUSINESS CASE 5

2.1 Project aims 5
2.2 Project unknowns 5
2.3 Budget spend constraints 6

3 PROJECT DESCRIPTION 7

3.1 Scope 7
3.1.1 Includes ("IN" Scope) 7
3.1.2 Excludes ("OUT" Scope) 8
3.1.3 Scope Statement 8
3.2 Success Criteria 9
3.3 Stakeholder and User Needs 10
3.4 Work Packages and Deliverables 11
3.5 Features 11
3.6 Constraints 12
3.7 Assumptions 12
3.8 Risks 13

4 COST, TIMING AND RESOURCES 15

4.1 Cost 15
4.2 Timing and Milestones 15
4.2.1 EU-FOSSA 2 Project Milestones 15
4.2.2 EU-FOSSA 2 Project Timing 16
4.3 Planned Resources 16

5 APPROACH 17

5.1 Methodology 17
5.2 Change Management 17
5.2.1 Project Change 17

6 GOVERNANCE AND STAKEHOLDERS 18

6.1 Project Steering Committee 18
6.2 Structure 18
6.3 Roles and Responsibilities 18
6.4 Other Stakeholders 19

1 EXECUTIVE SUMMARY

This section is an executive summary of the Project Charter for the EU-FOSSA 2 project.

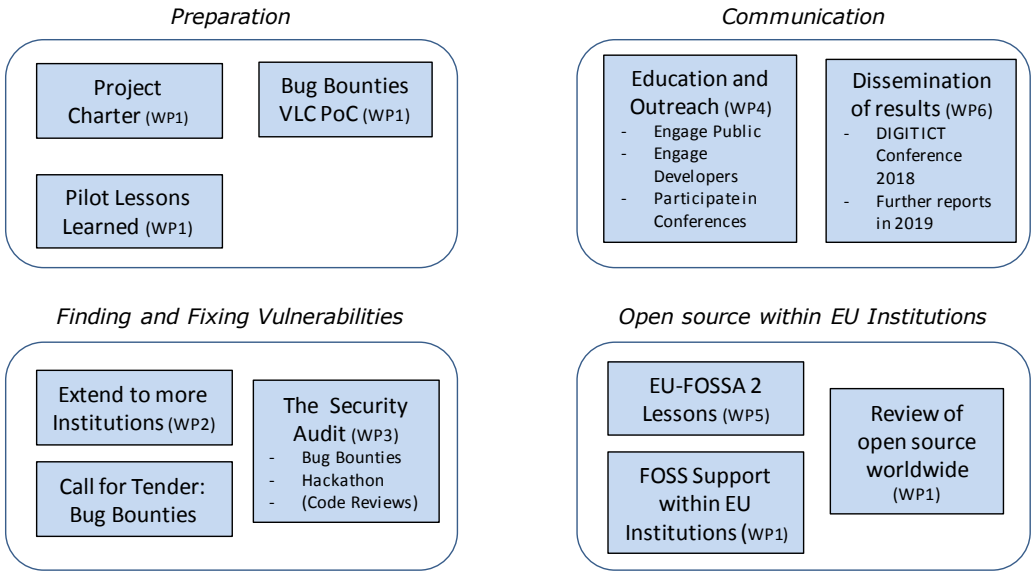
Project aims

EU-FOSSA was a pioneering and successful effort on a number of counts. EU-FOSSA 2 aims to go further and explore additional avenues to secure the FOSS that the EU institutions use. Specifically, it will:

- **Extend scope**: Extend the scope to additional EU institutions potentially allowing the increase of footprint of FOSS
- **Bug Bounties**: Use Bug Bounties as the primary method for conducting security audits, with possible code reviews in a backup role
- **Commonly used software**: Support open source projects relevant to the EU institutions and the general public and improve their security, by bringing together core developers from the institutions and the projects together in Brussels, where they can work together and fix security vulnerabilities. These exercises are called *developer conferences* or *hackathons*.
- **Developer/Public Engagement**: Engage wider with the public and developer groups to increase the awareness for software security and the general visibility of open source software used and relied upon within the institutions; and also understand current and planned initiatives within the community
- **Explore new methods**: Explore further tools/methods and conduct studies to make FOSS safer within the EU institutions, developer community and wider public

Work plan

The project team will focus on four key areas, and conduct work via nine well defined work packages. The diagram below shows the individual work packages.



Planned timescales

The table below shows the planned time scales for the work packages.

	2017												2018												2019						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	22	23	24	25	26	27	28	29	30
Months since start 2017	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
WP1: Preparation																															
WP1: FOSS Review																															
WP2: Extend Inventories to more institutions																															
WPX: Call for Tenders																															
WP3: The Security Audit																															
WP4: Education and outreach																															
WP5: Post EU-FOSSA 2																															
WP6: Dissemination of results																															
WP7: Dedicated PM																															
Contingency																															

Note: The preparation for the Call for Tenders did not have an allocated budget from EU-FOSSA, therefore no work package has been assigned to it, and it has been referred to as WPX.

Budget

		2017	2018	
Task	Work Package	Amount	Amount	Total cost
Preparation + OSS studies	WP1 (k€)	*43*	*207*	*250*
Extend Inventories	WP2 (k€)	*0*	*150*	*150*
The security audit	WP3(k€)	*0*	*1085*	*1085*
Education and outreach	WP4 (k€)	*0*	*500*	*500*
Post EU-FOSSA 2	WP5 (k€)	*0*	*100*	*100*
Dissemination of results	WP6 (k€)	*0*	*100*	*100*
Dedicated PM	WP7 (k€)	*127*	*288*	*415*
	Total (k€)	*170*	*2430*	***2600***
	FTE officials	*0.25*	*0.25*	

Key Challenges/Risks

- **Project**
    - Delay in the Call for Tenders can delay start of bug bounty programme creating a decision crunch in Q4 2018.
- **Budget**
    - Bug Bounties are unpredictable in terms of budgeting vs actuals spent
    - All funding to be **fully committed by 31 December 2018**, though invoices can arrive later. Given that December is a challenging months to obtain all approvals and signatures, the effective internal project deadline for budget re-deployments across project tasks, is really 1 December 2018.
    - The project team continues to explore other avenues to gain flexibility with inter-task budget deployment.

End of Executive Summary

2 CONSIDERATIONS ON THE BUSINESS CASE

This Project Charter has been developed for the EU-FOSSA 2 (Free and Open Source Software Auditing) preparatory action, which follows on from the pilot project EU-FOSSA. Its key objectives are to:

- Continue the work started in EU-FOSSA
- Extend the security audit to additional EU institutions
- Increase the visibility of open source software and how the EU institutions rely on it for their daily work whether in use or for the development of internal software; thus increase the awareness of how important open source software is for the EU institutions, developers and the general public
- Continue to raise awareness for the issue of security in open source software in light of the importance of open source, and help build "capacity and capability" for building and improving security *during* the development of open source software
- Ultimately make commonly used software safer for all groups of users

2.1 Project aims

The Project charter aims to:

- Outline the scope and success criteria of the project. Also describe the plan of work, dependencies, resources, assumptions, constraints and risks for the project
- Define the key work packages and deliverables within these work packages, and outline their target delivery dates
- Clearly indicate the costs at each stage and agree reporting and change management processes
- Outline the project governance plan

2.2 Project unknowns

Note: It is worth pointing out, that right from the outset, the project team is aware of a number of aspects of the project, which whilst they cannot be predicted, will shape the direction of the project. For example, some of these are:

- The degree of participation by EU institutions
- The degree of external developer and public engagement and reaction in relation to the efforts undertaken in communication and outreach
- The contents submitted in the inventories
- Which software will be submitted for further audit
- The success of the bug bounty programme in relation to the efforts undertaken in communication and outreach
- The need for and success of formal code reviews, should the bug bounty approach not yield good results

On the other hand, it is also worth noting, that this project stands on the experience of the Pilot EU-FOSSA project, and so the project team is familiar with one pass of the process. The one area that was not covered in the pilot was Bug Bounties and to alleviate that risk, EU-FOSSA 2 ran a proof of concept Bug Bounty project in December 2017, which proved successful, and provided many useful lessons for this larger Bug Bounty exercise.

2.3 Budget spend constraints

Due to the Commission's budget rules, the project is required to commit all its funding, via signed contracts, in the calendar year 2018. Any budgets not used, will be unavailable to the project from 1 Jan 2019.

This constraint is likely to present a challenge if the project wishes to engage different approaches or suppliers, based on the outcome of the first few stages of the project.

It is understood that post commitment, the supplier can submit invoices through 2019 and 2020.

3 PROJECT DESCRIPTION

3.1 Scope

The EU-FOSSA 2 preparatory action builds on the EU-FOSSA pilot project executed during 2015-2016 and intends to define a sustainable process of improving the security of Free and Open Source Software used in the European institutions.

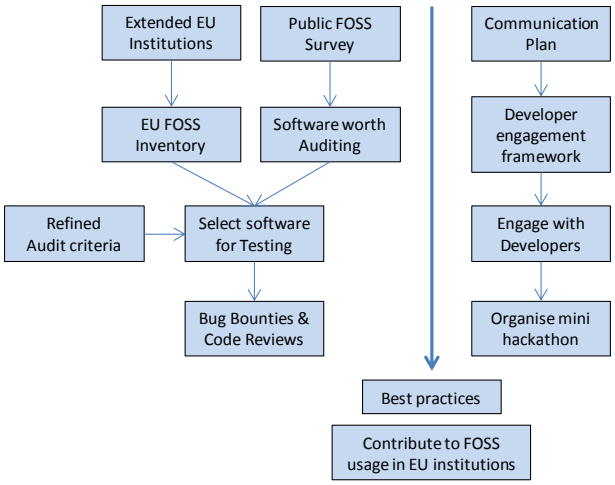
FOSSA stands for *Free and Open Source Software Auditing*. The high level objectives of both projects are:

- **Audit:** catalogue, assess and audit the FOSS used within the EU institutions
- **Raise awareness**: inform institutions, developer groups and the public about security threats
- **Make Safer**: support deeper vulnerability testing to make FOSS use safer for all stakeholders
- **Promote standards**: bring together key stakeholders and support the use of security standards

The specific scope of the EU-FOSSA 2 project is shown below, followed by items out of scope.

3.1.1 Includes ("IN" Scope)

The schematic below shows the key items of work for the project, and is followed by a description.



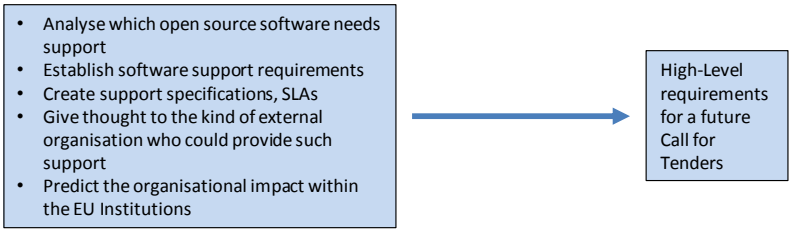
- **Extend participation**: extend the search for FOSS to additional Commission directorates and other EU institutions. The final participating group will be referred to as participating EU institutions;
- **Include tools**: in addition to software used in end-user contexts, for example on desktops or servers, include open source software development frameworks, tools and software, such as libraries built upon in software development and customization within the EU institutions, and examine software planned for introduction;
- **Public**: run a survey to learn about preferences of the general public for running security audits of open source software. We will then assess their candidature for vulnerability assessment, while remaining mindful of the main objective of raising awareness for and improving the security of FOSS used within the participating EU institutions. It is to be noted that whilst preparing all project deliveries, in particular the inventories, with the aforementioned objective of raising awareness in mind, they must be prepared for publication (this is without prejudice to understandable security and secrecy considerations the institutions may have regarding certain elements, such as for example: concrete software version numbers, lists of software installed on individual workplace PCs the list of PCs).
- **Select software for testing**: select candidates for deeper vulnerability testing for improved security at the EU institutions and general public;
- **Conduct the Testing**: conduct vulnerability assessment primarily via bug bounties, and based on the results, evaluate the additional benefit of select code reviews and where appropriate, conduct them;
- **Communicate**: initiate a communication plan to raise awareness for and improving the security of FOSS used within the participating EU institutions in the user and developer community, and

create a framework for engaging with the developer community; attend and speak at (if appropriate) limited and highly focussed open source related conferences and events;

- **Engage with Developers**: engage the FOSS developer community to inform them and gain their cooperation, encouraging a greater focus on security within the community and demonstrating the benefit of open source software to the EU institutions. Also, improve the security of commonly used open source software, organise small developer conferences/ hackathons to flush out and solve vulnerabilities in a closed setting;
- **Processes and documentation**: generate a set of supporting processes and documentation for the project, a developer engagement framework, a bug bounty management process and best practices for running bug bounties, and communication for the use of existing security best practices for developers and users;
- **Contribute to FOSS usage in EU institutions**: Whilst the project team will meet different groups and come across new ideas for making FOSS safer, it is also considered imperative that it continually reviews the use of open source software within the EU institutions and has a good understanding of open source usage across the world, in particular in public institutions

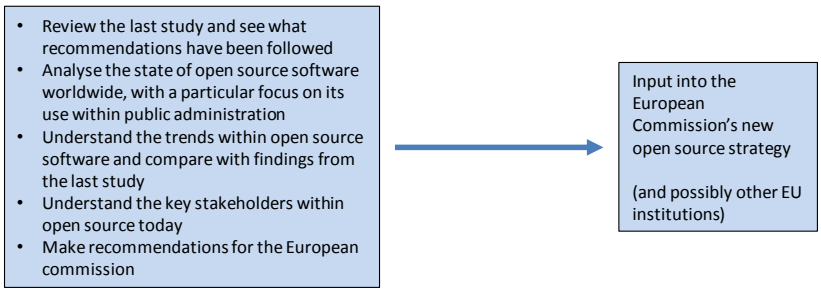
Initiative 1: Define support requirements for open source within the EU institutions

The boxes below show the key activities within the initiative and its chief output



Initiative 2: Review of the state of open source in the world today

The boxes below show the key activities within the initiative and its chief output



3.1.2 Excludes ("OUT" Scope)

EU-FOSSA 2 will not deal with:

- Proprietary and closed source software, that falls outside the definition of "Free and open source software".
- FOSS not used within EU institutions – software that does not show up in the inventories, with exception cases of software planned to be used in the future
- FOSS used by non-participating EU institutions
- Developing fresh security practices/guidelines to be used at the EU institutions

3.1.3 Scope Statement

The EU-FOSSA 2 preparatory action builds on the EU-FOSSA pilot project executed during 2015-2016 and intends to define a sustainable process of improving the security of free and open source software used in the European institutions, in particular by running bug bounties, code reviews and by engaging with the free and open source software communities.

In particular, the EU-FOSSA 2 project will audit the free and open source software used within the participating EU institutions; improve the safety of the most business critical software found by engaging the developer community and running bug bounties, code reviews and organising a hackathon specifically for under-funded but widely used software; and initiate a communication plan to raise awareness of cyber security best practices within the developer and user community and the role the EU is playing to improve the safety and security of widely used free and open source software.

3.2 Success Criteria

The success of the EU-FOSSA 2 preparatory action project can be judged by the following measurable criteria:

(i) Software related results – how many bugs found? Their level of criticality? Were they fixed, and if not, why not?

(ii) How the project engaged with the community – the developers and public – and how well the visibility of FOSS used within the EU institutions was raised

(iii) How well the project is run, from a project task execution and management perspective

(iv) Did it improve the uptake of and make it easier for free and open source software to be more widely used in the EU institutions

The 2nd aspect of engaging with the community is hard to measure and therefore challenging to use as a success criterion. However, given that it is clearly the raison d'être for the project, it must be accounted for. We have therefore created the table below which shows two tiers of project success.

EU-FOSSA 2 Results[1]

Area	Successful	Highly Successful
Extend audit participation	Other Commission directorates and another EU institution added	Commission directorates and several EU institutions added
Inventory completeness	Inclusion of tools in inventory	Inclusion of tools in inventories from added EU institutions
Inventory creation	Inventories could be published after redaction	Inventories were prepared with publication in mind
Inventory publication	Inventories published after Q1/2019	Inventories published by Q4/2018
Communication plan	Plan is created and executed	Good feedback from all stakeholders
Engage with Public	Survey conducted, responses reach at least number of responses of PP survey within a comparable timeframe	Positive public response and higher participation, feedback influencing the project
Engage with developers	Developers in open source projects recognize EU-FOSSA and have responded to outreach undertaken	High engagement, acceptance, positive feedback, and high participation rate
Raise FOSS visibility	Interested public recognises the use of FOSS in participating EU institutions	General public and EU institutions recognise how EU institutions use and rely on FOSS for internal development of services and software
Select software for testing	Inventories inform internal choice, internal selection with less successful public engagement	EU/world-wide recognition of selection
Bug finds	> 50% of bugs reported are recognised as bugs by participating projects	> 50% of bugs reported are recognised and the number of submissions is as big as in comparable bug bounties
Bug severity	> 25% of bugs recognised are of at least a moderate severity/impact	> 50% of bugs recognised are of at least high severity/impact
Run Bug Bounties	Successful bug finds, > 50% budget used by bug bounties and hackathons	Successful bug finds, > 75% budget use through bug bounties and hackathons
Bugs fixed, security improved	Projects give feedback that they could (or will) fix >25% of recognised bugs	Projects give feedback that bugs recognised were useful to identify security issues and indicate that they have fixed or will fix bugs
Conduct code reviews	Low need for code reviews	No need for code reviews
Arrange hackathons	One or more events arranged from Q4 2018, with participation from projects	One or more events arranged and project gives positive feedback as to the usefulness; participation from projects and staff from EU institutions
Processes and	All items created and published	Adopted and planned for use by EU

[1] following the definitions in 2 and 3.1**Error! Reference source not found.**

documentation		institutions
Explore new ways to make FOSS safer	Some new ideas emerge and are discussed as possible next steps	One-two ideas are fleshed out ready for action in the next stage of the EU-FOSSA project
Contribute to FOSS usage in EU institutions	Open source support needs defined and a successful study of the open source world trends	Output from the two studies result in buy-in from EU institutions about the strategic use of open source and its management.

EU-FOSSA 2 Openness

- Outcomes of the project will be published and disseminated outside the European institutions. They will be designed to be shared and to be used by other institutions, public entities and communities.
- External stakeholders such as developer communities and the EU public will be informed and are invited to participate in the project.

EU-FOSSA 2 Sustainability

- Following the pilot project and the current preparatory action, the EU-FOSSA project will have accumulated valuable insight on the scale of use of FOSS within the EU, the key threats faced and the process of managing/mitigating those threats. These will form input to the creation of best practices in managing FOSS within the EU.
- The methodologies defined during the project will be practical and ready to be used by other European institutions and directorates, ideally with a benefit to further public entities throughout the EU.

3.3 Stakeholder and User Needs

The Stakeholders identified during the EU-FOSSA pilot project are:

Stakeholder	Role
DIGIT.B3	Internal Stakeholder
DIGIT.B	Internal Stakeholder
DIGIT	Internal Stakeholder
EC Infrastructure, IT Security and Development	Organisation Stakeholder
Other participating EU institutions' IT functions	Organisation Stakeholder
European Parliament MEPs	Organisation Stakeholder
FOSS Developer groups (specific groups to be agreed)	External Stakeholder
EU Public	External Stakeholder

The needs to be addressed in the EU-FOSSA 2 project are shown below:

ID	Need Description	Priority
N1	Extend the scope of the project to more Commission Directorates and EU institutions	1
N2	Create a fresh inventory of FOSS of the expanded EU institutions	1
N3	Refine and further develop the criteria for an EU software and projects auditing framework	2
N4	Create an infrastructure to encourage engagement with FOSS developer communities, to aid the discovery of security bugs and raise awareness about software security in general	1
N5	Create a framework for engagement with the EU Public on issues of software security	2
N6	Improve security and guard against future threats by conducting bug bounties and where necessary, code reviews, to detect and fix potential security vulnerabilities	1
N7	Document processes and create a framework to manage FOSSAs on an ongoing basis	1
N8	Contribute to FOSS usage in EU institutions	1

3.4 Work Packages and Deliverables

ID	Work Package/Deliverable	Deliverable Description
WP1	Preparation	
D1.1	- Project charter	- A Project Charter document for the project
D1.2	- bug bounties Proof of concept (PoC)	- BB PoC Report
D1.3	- lessons learned from the EU-FOSSA pilot	- Lessons learned document
D1.4	- Define support requirements for FOSS usage within the EU institutions	- A detailed report describing the EU Institutions' FOSS support requirements potential solutions, and specifications for work, which would feed into a future call for Tender.
D1.5	- Review of the FOSS world	- A report of the status of FOSS in the world today compared with the last such report, with particular focus on FOSS usage within Public institutions and FOSS trends. This information will be a useful basis for deciding the wider EC OSS strategy review.
WP2	Extend Inventories to more institutions	
D2.1	- Improved inventory collection methodology	- An improved unified methodology to build/update (periodically or continuously) inter-institutional inventory of software and tools.
D2.2	- Inventory list	- The final list of existing and planned FOSS software, development frameworks, standards, tools and libraries
D2.3	- Rationale and list of security audit software	- the rationale and list for selecting software for audit
D2.4	- Publication of inventories	- A document for public consumption
WP3	The Security Audit	
D3.1	- Bug Bounties (BB)	- BB findings summary report
D3.2	- Code Reviews (CR)	- CR findings summary report
D3.3	- Hackathons	- Hackathon results summary report
D3.4	- Additional approaches to make FOSS safer	- explored options for post EU-FOSSA 2
WP4	Education and outreach	
D4.1	- An overall project communication plan	- A comprehensive plan to engage with all stakeholders
D4.2	- A public software security engagement survey	- Public engagement survey results
D4.3	- Developer engagement	- Actual developer engagement based on a planned developer engagement plan.
WP5	Post EU-FOSSA 2	
D5.1	- EU-FOSSA 2 Lessons learned	- A summary of the lessons learned from the project
D5.2	- EU-FOSSA processes and management	- EU-FOSSA Processes and guidelines for managing future projects
WP6	Dissemination of results (Conference)	
D6.1	- Dissemination of initial results at the DIGIT ICT 2018 conference - Further dissemination in 2019	- A management presentation and a report, including feedback from involved FOSS projects
WP7	Dedicated Project Manager	
D7.1	- Dedicated Project Manager	- A dedicated PM to handle the project

3.5 Features

Need	Features	Deliverables
N1	**Increased participation in inventories**: a larger number of EU institutions will hold a stake in the safety of FOSS they use	D2.1 & D2.2
N2	**Transparent inventory list**: can be seen within the EU and publicly (except sensitive data), and analysed	D2.2
N2	**Well defined Inventory methodology**: current and upcoming FOSS software, associated development tools, frameworks and libraries.	D2.1
N2	**EU FOSS Inventory**: The inventory and metrics relating to it will allow the EU institutions to understand what FOSS exists and where, its level of security and impact of a security attack	D2.2

N3	**Improved software selection method**: An improved method for the identification of software which requires further security testing (based on vulnerability/impact on the EU)	D2.1
N3	**Vulnerability assessment process**: A well-defined process for the EU to manage vulnerability testing via bug bounties and code reviews	D5.2
N4	**Framework for developer engagement**: proven framework for engagement with Developer groups for FOSS vulnerability awareness, assessment and best practices.	D4.3
N5	**Public engagement**: the project will allow a direct contact with the public, via a survey and via feedback mechanisms	D4.2
N6	**Developer hackathon blueprint**: A blueprint for arranging developer conferences to solve bugs in commonly used FOSS	D5.2
N6	**Safer software**: Thorough having higher risk software vulnerability tested	D3.1, D3.2 & D3.3
N6	**Increased adoption of best practices**: by the EU institutions, the developer community and the general public	D4.1, D4.2 & D4.3
N7	**Processes and documentation**: with particular focus on the software audit criteria; developer engagement framework, bug bounty management process, and communication for the use of existing security best practices for developers and users.	D5.2
N7	**Vulnerabilities reporting process**: the process to report vulnerabilities needs to be defined involving the end users. In OSS security governance, the systems' end users play an important role in finding new vulnerabilities.	D5.2
N8	**Open source within the EU institutions:** study the worldwide state of open source and create support mechanisms for greater EU institutional use	D1.4, D1.5

3.6 Constraints

The EU-FOSSA 2 project foresees the following constraints:

- The entire budget must be committed in 2018.
- To achieve this, the project will have to adhere to a strict timetable commencing with the Call for Tender being issued in April 2018.
- The execution of the project is expected to continue well into 2019, and it will only be possible to provide an interim report during the DIGIT ICT 2018 conference on 20th of November 2018. The DIGIT ICT 2019 will also be a good forum for updates, but could be too late, if it is to play a part in approving the transition from preparatory action project to a permanent action project. Therefore additional updates will be provided via other means throughout 2019.
- The project is highly dependent on the cooperation, proactive and timely communication [*] on all project steps, as well the engagement of all involved from both the European Parliament and the European Commission.
- **Note**: [*] as agreed at the first meeting of the project's steering committee on 14 March 2018, the Commission will keep the Parliament informed of next steps to be communicated and/or acted on with at least two weeks' notice to give all sides enough time to prepare communication etc.

3.7 Assumptions

The project makes the following assumptions

1. The European Commission and the European Parliament will work together to ensure the success of the project
2. The additional participating EU institutions will cooperate in supplying the requested information to the project

3. WPX (Call for tenders) starts in **April 2018**, and after all approvals, the large scale Bug Bounty part will start in August 2018. Any delay in this timetable could negatively impact the project.

3.8 Risks

ID	Risk Description & Details	Status	Likelihood[2]	Impact[3]	Risk Level[4]	Risk Owner	Risk Response Strategy[5]	Action Details
1	The quality of the deliverables may not be up to the required standards, hindering the project from progressing or completing.	Detected	M	H	H	PM / PO	Reduce	The project team will review the quality of deliverables along the way and due to a series of backup options, change tack as needed.
2	Not enough EU institutions participate (WP2) leading to a lost opportunity for improving EU Security	Detected	M	L	L	PM / PO	Avoid	Additional Institutions have already expressed interest
3	Institutions do not furnish the required information (WP2) in adequate detail	Detected	L	M	M	PM / PO	Reduce	There is a well proven automated methodology from the Pilot stage of EU-FOSSA, which will allow a certain amount of data. We also have lessons learned from last time which will help.
4	There may be no consensus between stakeholders in the selection of software for further security audit	Detected	H	H	H	PM / PO	Accept	Requirements of the selected components will be defined at the beginning of the project based on objective, measurable criteria, such EU impact and sustainability.
5	Non critical software is put forward for Audit (WP2)	Detected	L	H	H	PM / PO	Avoid	The above methodology will automatically flush out low impact software.
6	Call for tender issuance is delayed	Detected	L	H	M	PM / PO	Accept	The CfT is already delayed by one month. We have to plan to speed up internal approvals.
7	Call for tender internal EU approval is delayed to after September 2018	Detected	M	H	H	PM / PO	Reduce	We can mitigate against this by building flexibility into the CfT programme to allow it to continue to end 2019.
8	Call for tender results are unsatisfactory	Detected	L	M	M	PM / PO	Reduce	The likelihood of this is low, because we have already worked with one competent company in the pilot, and there are others in the marketplace who have expressed an interest. We will also aim to create a framework contract, which would allow us to hedge against just one supplier.
9	Bug Bounties do not find enough high quality bugs (WP3)	Detected	M	M	M	PM / PO	Accept	This is a real risk and does not in itself reflect badly on the project exercise. We will mitigate against this via alternative solutions, via code reviews.
10	Many code reviews are needed due to unsatisfactory results from the Bug Bounties (WP3)	Detected	M	M	H	PM / PO	Accept	This is a realistic possibility, and planned for.
11	The code reviews may not bring valuable results to develop the security assessment.	Detected	L	H	M	PM / PO	Reduce	A Result report will be defined at the beginning to be sure about the results required and its meaning.
12	The developer conference/ hackathon proves to be unproductive (WP3)	Detected	L	M	M	PM / PO	Reduce	The risk can be mitigated by extensive involvement with the developer communities and selecting the right software
13	Developer engagement proves unproductive (WP4)	Detected	L	L	M	PM / PO	Reduce	We aim to replicate and hopefully improve upon the pilot project's engagement, which proved to be highly productive.
14	Public support for EU-FOSSA is unenthusiastic (WP4)	Detected	L	L	M	PM / PO	Reduce	We aim to replicate and hopefully improve upon the pilot project's engagement, which proved to be highly productive.
15	Stakeholders may not be engaged properly along the entire project.	Detected	M	H	H	PM / PO	Reduce	Communication and dissemination plans will be designed from the outset to deal with this. Stakeholders will be require to validate the outputs of all the WPs.
16	It is not possible to carry forward the budget for the conference to 2019	Detected	M	H	H	PM / PO	Accept	The project will plan around this.
17	The Project Manager may leave or be unfit for purpose	Detected	L	M	M	PM/PO	Reduce	The manager of the PM can step in and complete the job.
18	The inertia of the European institutions may make it	Detected	M	H	H	PM / PO	Reduce	WP7 will be continuously monitoring the project planning to assure main milestones. They will be

[2] A numeric value denoting the relative probability that the risk should occur.
[3] A numeric value denoting the relative severity of the impact of the risk if it should occur.
[4] The risk level is the product of the likelihood and impact (RL=L*I).
[5] The possible risk response strategies are: Avoid/ Transfer or Share/ Reduce / Accept.

ID	Risk Description & Details	Status	Likelihood[2]	Impact[3]	Risk Level[4]	Risk Owner	Risk Response Strategy[5]	Action Details
	difficult to finish the project on time (time to hire consultants, time to gather data, time to sign contracts, time to organise meetings, time to collect approvals …). (1)							in charge of planning changes when necessary. Involve top management when roadblocks are encountered.
19	Publishing of inventory information is held up due to perceived sensitivity of data	Detected	M	L	M	PM / BM / PO	Avoid	WP2 will from the outset aim to collect data in a format which is easy to publish and any sensitive data redacted.
20	Publishing of inventory information is held up due to internal bureaucracy	Detected	M	L	L	PM / BM / PO	Avoid	WP2 will from the outset aim to collect data in a simple pre-agreed format.

Likelihood: (H) High probability; (M) Medium probability; (L) Low probability.

Impact: (H) High impact; (M) Medium impact; (L) Low impact.

Risk level: (H) High; (M) Medium; (L) Low.

4 COST, TIMING AND RESOURCES

4.1 Cost

Commitment appropriations for this preparatory action (Budget line 26 03 77 06) were voted for the first year under the 2017 Budget.

It follows a pilot project (Budget line 26 03 77 02), for which commitment appropriations were voted under the 2015 Budget.

		2017	2018	
Task	Work Package	Amount	Amount	Total cost
Preparation + OSS studies	WP1 (k€)	*43*	*207*	*250*
Extend Inventories	WP2 (k€)	*0*	*150*	*150*
The security audit	WP3(k€)	*0*	*1085*	*1085*
Education and outreach	WP4 (k€)	*0*	*500*	*500*
Post EU-FOSSA 2	WP5 (k€)	*0*	*100*	*100*
Dissemination of results	WP6 (k€)	*0*	*100*	*100*
Dedicated PM	WP7 (k€)	*127*	*288*	*415*
	Total (k€)	*170*	*2430*	***2600***
	FTE officials	*0.25*	*0.25*	

4.2 Timing and Milestones

4.2.1 EU-FOSSA 2 Project Milestones

ID	Milestone Description	Target Delivery Date
WP1	Preparation	
D1.1	- Project charter	End Jan 2018
D1.2	- Bug bounties Proof of Concept (PoC)	8 Jan 2018
D1.3	- Lessons learned from the EU-FOSSA pilot	Mid Feb 2018
D1.4	- Define support requirements for FOSS usage within the EU institutions	Apr 2018 – Nov 2018
D1.5	- Review of the FOSS world	Apr 2018 – Nov 2018
WP2	Extend Inventories to more institutions	
D2.1	- Improved inventory collection methodology	End Feb 2018
D2.2	- Inventory list	End Apr 2018
D2.3	- Rationale and list of security audit software	End Jun 2018
D2.4	- Publication of inventories	From Q4/2018
WP3	The Security Audit	
D3.1	- Bug Bounties (BB)	Aug 2019
D3.2	- Code Reviews (CR)	Aug 2019
D3.3	- Hackathon	Q4 2018
D3.4	- Additional approaches to make FOSS safer	Q2 2019
WP4	Education and outreach	
D4.1	- An overall project communication plan	Mar 2018-Sep 2019
D4.2	- Public engagement and survey	Mar 2018-Sep 2019
D4.3	- Developer engagement	Mar 2018-Sep 2019
WP5	Post EU-FOSSA 2	
D5.1	- EU-FOSSA 2 Lessons learned	Sept 2019
D5.2	- EU-FOSSA 2 processes and management	Sept 2019
WP6	Dissemination of results (Conference)	
D6.1	- Dissemination of results at the DIGIT ICT 2018 conference and later on an ongoing basis	Dec 2018 - Sep 2019
WP7	Dedicated Project Manager	
D7.1	- Dedicated Project Manager	Dec 2017 - Oct 2019

4.2.2 EU-FOSSA 2 Project Timing

The table below shows a high level project time plan based on the key deliverables within a work package.

EU-FOSSA 2 Overall Planning	Months since project start in June 2017																														
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M22	M23	M24	M25	M26	M27	M28	M29	M30
Months	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
WP1: Preparation																															
D1.1 Project Charter																															
D1.2 Bug bounties Proof of concept (PoC)																															
D1.3 Lessons learned from the EU-FOSSA Pilot																															
D1.4 Define FOSS support for EU institutions																															
D1.5 Review of the FOSS world																															
WP2: Extend Inventories to more institutions																															
D2.1 Improved collection methodology																															
D2.2 Inventory list																															
D2.3 Rationale and list of security audit software																															
WPX: Call for Tenders																															
X.1 Tender for the Bug Bounty programme																															
X.2 Supplier list for code reviews																															
WP3: The Security Audit																															
D3.1 Bug Bounties (BB)																															
D3.2 Code Reviews (CR)																															
D3.3 Hackathon																															
WP4: Education and outreach																															
D4.1 An overall project communication plan																															
D4.2 Public engagement and survey																															
D4.3 Developer engagement																															
WP5: Post EU-FOSSA 2																															
D5.1 EU-FOSSA 2 Lessons learned																															
D5.2 EU-FOSSA processes and management																															
WP6: Dissemination of results (Conference)																															
D6.1 At the DIGIT ICT 2018 conference and later																															
WP7: Dedicated Project Manager																															
D7.1 Dedicated project manager																															
Contingency																															

Note: The preparation for the Call for Tenders did not have an allocated budget from EU-FOSSA, therefore no work package has been assigned to it, and it has been referred to as WPX.

4.3 Planned Resources

This project is intentionally light on internal resources, as the execution work is all outsourced to internal EU departments or externally contracted organisations. The main project resource is the Project Manager who will manage the external parties and coordinate the work.

5 APPROACH

5.1 Methodology

The Commission's PM^2 methodology will be applied, which defines ownership, roles, governance, interaction and share of responsibilities between IT and business, change and control management. The application of PM^2 ensures that benefits will be achieved within predictable time, cost, scope, risk and quality.

5.2 Change Management

Change management follows PM^2 methodology. Changes are decided by the Project Steering Committee consisting of Project Owner/Business Manager and Solution Provider/Project Manager.

5.2.1 Project Change

The following change requests will be managed according to the standard PM^2 Scope and Change Management Plan:

- Project scope change.
- Dates of milestones.
- Changes to contracted professional services (e.g. additional consulting visits)
- Additional project spending.

The change control procedure for stakeholder reported issues will be:

1) **Captured**: determine issue type (change requests, off-specifications, new risks, questions, concerns, good ideas etc.), determine severity and register the issue
2) **Examined**: assess the impact of the registered issue on the project's objectives and project's risks
3) **Proposals**: identify, evaluate and prioritise, or recommend options
4) **Decide**: escalate if beyond authority, approve, reject or defer
5) **Implement/rejected**: execution of the final decision

6 GOVERNANCE AND STAKEHOLDERS

6.1 Project Steering Committee

The EU-FOSSA 2 project will have a Project Steering Committee (PSC) including representatives of the European Parliament and the European Commission.

(personal data removed for publication)

6.2 Structure

The EU-FOSSA 2 project follows PM^2 assignment of Roles and Responsibilities. Figure 1 describes the proposed organizational structure. For names, refer to the makeup of the Project Steering Committee:

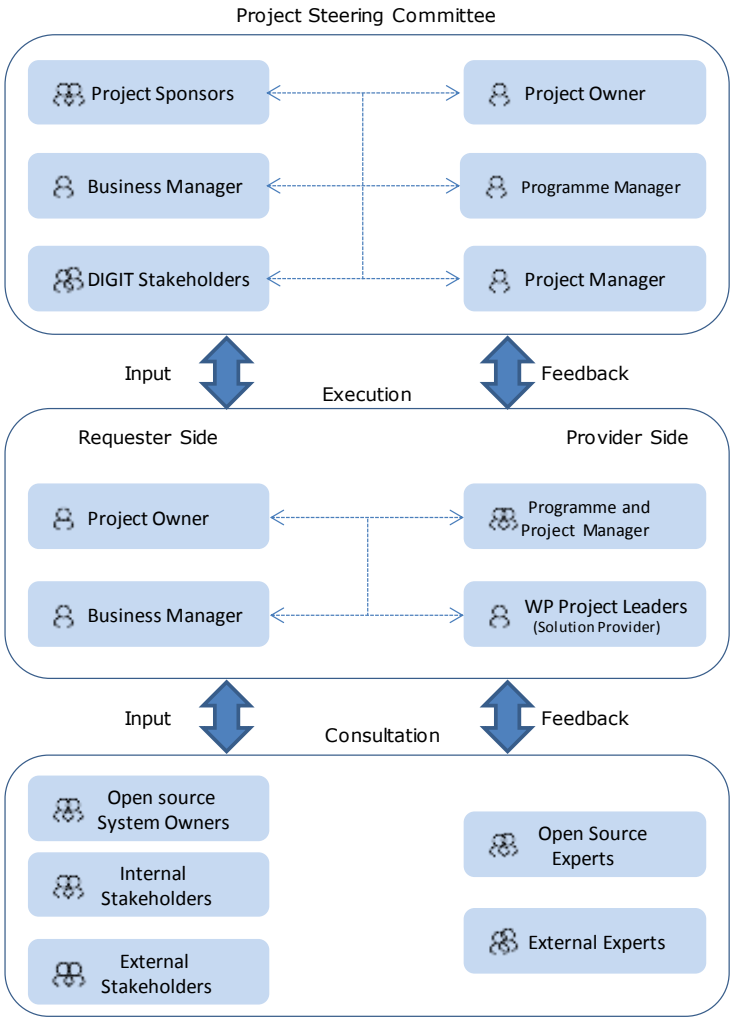


Figure 1 – Governance of the EU-FOSSA 2 Preparatory Action Project

6.3 Roles and Responsibilities

The following table describe the responsibilities of the PM^2 roles identified.

IT Governance body	Role and Responsibilities
Project Steering Committee	Sets direction for the project and steers the project through any major issues the project team faces.
Business Manager	To provide the business input to the project, by acting as the representative of the project sponsors at an operational

	level. To interpret and clarify any business questions and directional issues to the project team, which do not need a PSC review. To promote alignment between stakeholders and the project mandate.
Project Owner	Owns the Project, from a project delivery perspective, and is ultimately responsible to the Project Sponsors. To initiate the project and manage it at a high level during its lifecycle. Support in the engagement of stakeholders. To approve any project changes.
Programme Manager	To guide the Project Manager in his/her day to day activities.
Project Manager	To lead and follow-up the project. To manage the WPs contractors. To assure the project is aligned with the business case and the project charter. To manage project changes, to update the planning and anticipate the risks.
WPs Project leaders – Solution Provider	To execute the tasks defined in the WPs. To report advances, risks and problems to the project manager.
Open source System Owners	Owners of the systems which will be searched, catalogued and audited – they will advise and assist in the inventory collection exercise.
Internal Stakeholders	To provide feedback regarding the results of the WPs.
Organization Stakeholders	To provide feedback regarding the results of the WPs.
Free and Open Source Software Experts	To provide best practices information. To help WPs contractors to create the mechanisms to let European Commission to contribute to free and open source communities.
External Experts	To give external and unbiased advice regarding the results of the WPs.

For additional responsibilities, please consult the PM^2 Methodology.

6.4 Other Stakeholders

Other stakeholders may be involved if approved by the Project Steering Committee.