EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate B - Digital Business Solutions
DIGIT B3 - Reusable Solutions

EU-FOSSA 2

WP5 D5.1 Final Report, Lessons Learned, and Outlook for Continuation

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: MO15 06/P010 - Tel. direct line +32 229-57084

Commission européenne, 2920 Luxembourg, LUXEMBOURG - Tel. +352 43011

saranjit-singh.arora@ext.ec.europa.eu

Table of Contents

1. INTRODUCTION

EU-FOSSA 2 (EU Free and Open Source Software Auditing) was a Preparatory Action no. 26.03.77.06 run during 2017-2020. It was a continuation of the successful EU-FOSSA Pilot Project (26.03.77.02).

Note: For legislation governing Pilot Projects and Preparatory Actions, please refer to a summary in "Pilot projects and preparatory actions in the annual EU budgetary procedure" [PilPr] and the EU Financial Regulation Article 58(2) [FinReg].

1.1. Purpose of the document

This document serves multiple purposes, it:

1. Lists what the project achieved and how successfully
2. Outlines the lessons learned by the project as a whole and for each work package
3. Assesses the impact of the project, both internally and externally
4. Provides thoughts on the continuation of the *essence of the project* via other initiatives
5. Acts as a final project report

1.2. Perspectives - Project Level and Work Package Level

This document provides two views, one from the overall project level (Chapter 2) and from a work package level (Chapter 3 onwards). For a quick overview, it is sufficient to read Chapter 2. The table below shows what is included at which level.

Information	Project level	Work-package level
Summarise key activities (where not evident or shown elsewhere)		✓
List deliverables	✓	
Evaluation of success criteria[1]	✓	
Lessons Learned	✓	✓
Experience with Suppliers		✓
Impact Analysis	✓	
Financial Summary	✓	

Note: To avoid duplication, material present in other documents is appropriately referenced.

[1] The success criteria for the project were defined in detail in the project charter, which is stored on Joinup.

2. PROJECT LEVEL SUMMARY

This section provides an overview of the entire project covering:

1. Financial summary
2. Statement of deliverables
3. Meeting the core objectives
4. Measurement against the Success criteria
5. Key lessons learned
6. The Impact (internal and external)
7. Outlook for the future

For an individual work package (WP) perspective, please see the relevant chapter below.

2.1. Financial Overview

The table below shows the financial spend on EU-FOSSA 2.

#	Work package	Original approved budget	Budget plans in project charter	Final budget allocation
WP1	Preparation and OSS review	250,000.00 €	250,000.00 €	257,945.00 €
WP2	Extend inventories	200,000.00 €	150,000.00 €	124,365.00 €
WPX	Call for Tenders	0.00 €	0.00 €	0.00 €
WP3	Security audit	1,100,000.00 €	1,085,000.00 €	1,156,069.67 €
WP4	Education and outreach	500,000.00 €	500,000.00 €	476,000.00 €
WP5	Post EU-FOSSA 2	100,000.00 €	100,000.00 €	0.00 €
WP6	Dissemination of results	150,000.00 €	100,000.00 €	0.00 €
WP7	Project Management	300,000.00 €	415,000.00 €	514,140.00 €
Totals		**2,600,000.00 €**	**2,600,000.00 €**	**2,528,519.67 €**

Budget Notes:

1. WPX did not have an EU-FOSSA budget and was part of DIGIT procurement
2. WP5 and WP6 were handled internally the EU-FOSSA 2 team by enlarging WP7

2.2. Project Deliverables

The table below shows the deliverables indicated in the project charter. Of these, two proved unnecessary, and therefore the project delivered all its deliverables.

ID	Work Package/Deliverable	Deliverable Description	Delivered (Y/N)
WP1	Preparation		
D1.1	- Project charter	- A Project Charter document for the project	Yes
D1.2	- Bug bounties Proof of concept (PoC)	- BB PoC Report	Yes
D1.3	- Lessons learned from the EU-FOSSA pilot	- Lessons learned document	Yes
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.	Yes
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.	Yes
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.	N/A[2]
D2.2	- Inventory list	- The final list of existing and planned FOSS software, development frameworks, standards, tools and libraries	Yes
D2.3	- Rationale and list of security audit software	- The rationale and list for selecting software for audit	Yes
D2.4	- Publication of inventories	- A document for public consumption	Yes
WP3	The Security Audit		
D3.1	- Bug Bounties (BB)	- BB findings summary report	Yes
D3.2	- Code Reviews (CR)	- CR findings summary report	N/A[3]
D3.3	- Hackathons	- Hackathon results summary report	Yes
D3.4	- Additional approaches to make FOSS safer	- explored options for post EU-FOSSA 2	Yes
WP4	Education and outreach		
D4.1	- An overall project communication plan	- A comprehensive plan to engage with all stakeholders	Yes
D4.2	- A public software security engagement survey	- Public engagement survey results	Yes
D4.3	- Developer engagement	- Actual developer engagement based on a planned developer engagement plan.	Yes
WP5	Post EU-FOSSA 2		
D5.1	- EU-FOSSA 2 Lessons learned	- A summary of the lessons learned from the project	Yes
D5.2	- EU-FOSSA processes and management	- EU-FOSSA Processes and guidelines for managing	Yes[4]

2 The current inventory methodology worked fine and did not need any modification

3 The project team decided that code reviews would not be conducted. This is because the bug bounties as an instrument, by virtue of the proof of concept, proven their effectiveness and superiority over code-reviews in finding bugs. Furthermore, the hackathons were expected to (and did) assist in finding further software vulnerabilities.

		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	Yes Yes
WP7	Project Management		
D7.1	- Dedicated Project Manager	- A dedicated PM to handle the project	Yes
D7.2	- Project Steering Committee meetings	- Holding regular project steering committee meetings	Yes[5]

2.3. The EU-FOSSA Programme Core Objectives

The high-level objectives of both the pilot EU-FOSSA and the preparatory action EU-FOSSA 2 projects were:

- **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

Note: There is widespread internal and external agreement that the EU-FOSSA programme successfully met these high-level objectives. The section below provides specific supporting evidence.

Figure: A schematic designed by the EU-FOSSA 2 communication team

Source: https://Joinup.ec.europa.eu/collection/open-source-observatory-osor/news/contribution-open-source-t

---

[4] This is an internal document and is not published.

[5] Meeting minutes are also internal project documents.

2.4. EU-FOSSA 2 Specific Objectives

The project's specific objectives were stated in the Project Charter document (see Joinup link https://Joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliverables).

EU-FOSSA 2 Objective	Was the objective achieved? If so, how?
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;	Yes. The project team reached out to a number of European institutions and had discussions with the European Parliament, Council of Europe, Council of the European Union, European External Action Service, European Economic and Social Committee and Committee of the Regions and the European Investment Bank. Most of these institutions shared their open source experiences and provided input, which was considered for the final selection of software for the bug bounties. Further, the European Council went a step further and opted to conduct their first inventory exercise for the FOSS they use. This initiative was financed by the EU-FOSSA 2 project.
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;	Yes. This time open source tools were included using the Nexus Data[6]. However, *software planned for introduction* was not included, as it was information that proved difficult to obtain via emails and questionnaires.
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;	Yes. The earlier EU-FOSSA pilot project survey had asked this question specifically and replies were captured in a free text field. After examining this, the project found a rich set of suggestions and so, it was decided by the steering committee that a fresh survey was not required. Public preferences were taken into account.
Select software for testing: select candidates for deeper vulnerability testing for improved security at the EU institutions and general public;	Yes. A shortlist was made based on a wide number of factors, including criticality of software, suggestions by the public, suggestions from other participating European institutions, a balance of front-end, middleware and server software, finally whether the software was recently tested

[6] Nexus Repository is an open source software repository that supports many artifact formats, including Docker, Java™, and npm. For more information regarding Nexus please see: https://www.sonatype.com/nexus-repository-oss

	by another organisation and the cooperation of the open source community.
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;	Yes. Fifteen (15) bug bounties were conducted with good results. Hence, no code reviews were required. For additional information on the criteria to perform code reviews please refer to EU-FOSSA 2 project charter. In section 1, executive summary it states "*Use Bug Bounties as the primary method for conducting security audits, with possible code reviews in a backup role*"
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;	Yes. A comprehensive communication plan was created and executed using a range of channels including twitter, press releases, speaking at open source conferences, spreading awareness via the hackathons and subsequent articles, press coverage via the European and global press. Specifically an end of year event organised jointly with DG Connect was held in November 2019 - **Open Source beyond 2020**, *Powering a Digital Europe* addressed open source software and hardware in Europe. A wide selection of people from across the open source spectrum attended.
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;	Yes. This core objective was met using many of the mechanisms mentioned on the left. The team and a number of key developers from European institutions met developers from across the world at events such as FOSDEM, the Apache, Linux, Paris and SuperSEC open source conferences in 2018 and 2019, DIGITEC 2018 and the three Hackathons organised as part of the EU-FOSSA 2 project. In addition, we organised video calls with around 6 micro open source communities. This engagement resulted in an increased understanding of the issues the open source community faces, in addition to finding and fixing security and other vulnerabilities.
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;	Yes. There are a number of initiatives and documents which collectively meet this objective. This lessons learned document is one such, and describes pitfalls to avoid and best practices to consider. In addition, we have retained and passed on experience arising from this project for future projects. Further, a framework contract for running bug bounties outside of the EU-FOSSA project is in place, for use until 2 October 2021 and can be extended. The Inventory methodology is in place and new pathways have been opened for engaging with open source communities via contacts made at hackathons, open source conferences etc.
Contribute to FOSS usage in EU institutions: Whilst the project team will meet different groups and come across	Yes. The project has undoubtedly raised the profile of FOSS across the European institutions.

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	This has led to a FOSS inventory exercise at the European Council, and a number of initiatives in other institutions. The numerous events the team attended along with participation in the Global FOSS study, helped the team to understand open source trends across Public Service bodies and leading private companies across the world.

2.5. Meeting the 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 did the project run from a task execution and management perspective
(iv) Did it improve the uptake of FOSS in EU institutions

The project charter listed two tiers of project success. The Success Criteria achieved has been marked in **bold** and shaded in green.

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[7]
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[8]	> 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**

7 This proved to have been an unrealistic success criteria, as the data for the inventories was from Dec 2018.

8 The success criteria for the bug bounties were set without prior industry or benchmarking experience. The usual success rate varies from 15-25% of bugs found, and from that metric, the bug bounties were *highly successful*.

		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 documentation	**All items created and published**	Adopted and planned for use by EU 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 results in buy-in from EU institutions about the strategic use of open source and its management.**

2.6. Impact Analysis

This section summarises the impact the project had on various stakeholders and entities.

2.6.1. Results and Impact on the European Commission

- **Safer FOSS**: The EU institutions and the open source ecosystem, now has safer open source software as a result of the EU-FOSSA initiative.
- **Open source thinking**: The EU-FOSSA 2 preparatory action intensified the Commission's thinking on its relationship with open source. The projects involved officials across many Directorates-General. Apart from the project owner, DIGIT, the project involved high level officials and key project officers at the cabinet level, CNECT, TAXUD, RTD, GROW, JRC, EMPL, HR, SCIC and others.
- **Value of open source**: This has deepened the Commission's understanding of the value of open source. More officials began considering the values of and differences between using of and contributing to open source, and considered their responsibilities as stewards. Very practically, the project revitalised and energised the Commission's thinking about open source.
- **Open source strategy**: Directly, it underpins the Commission's 2020-2023 Open Source Strategy (to be announced). Here it helped form principles and actions on the increasing use of open source, contributing back to open source, and organising the involvement with communities. Effectively, for DIGIT and therefore the Commission, EU-FOSSA 2 led to a ***bolder open source strategy***.
- **Security toolkit**: We now have a proven security toolkit, which can be used repeatedly – e.g. at other institutions such as the European Council and European Parliament.
- **DG Connect**: The study EU-FOSSA 2 study on open source has likely influenced the DG Connect "Study on the impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy", a Smart Study announced in 2019 and kicked-off in early 2020.
- **Open source communities**: The Commission's knowledge of the European open source software landscape and the communities' issues has deepened. Some of the observations can be seen in this chapter below.
- **Potential EC leadership role**: There was an overwhelmingly positive reaction from the open source community of the EU's involvement in open source and particularly in the hackathons.

2.6.2. Impact on the European institutions

- The project interacted with the following European institutions - European Parliament, Council of Europe, Council of the European Union, European External Action Service, European Economic and Social Committee and Committee of the Regions and the European Investment Bank.
- Naturally, each institution is at a different stage of FOSS usage and maturity. Without exception, every institution was enthusiastic about open source and its use within their organisation.
- The European Council's take up of the EU-FOSSA project's offer to conduct an inventory and analysis of their FOSS.
- Further, the Council is considering using the DIGIT's open source strategy as a template.
- Due to the close working with the MEPs, there was a wider effect of influencing other MEPs interested in the subject matter. Some of these MEPs are now supporting the project.

2.6.3. Impact on the Open Source Community

- The collaboration between the European Parliament and the European Commission also helped to create a visible buzz at project milestones - one of the reasons of the successful outreach to open source communities, the general public, IT trade press and general media.
- Open source leaders have actively contacted the project, by email, but also at presentations and conferences (FOSDEM, ApacheCon Europe, Linux Open source Summit Europe, Paris Open Source Summit etc.)

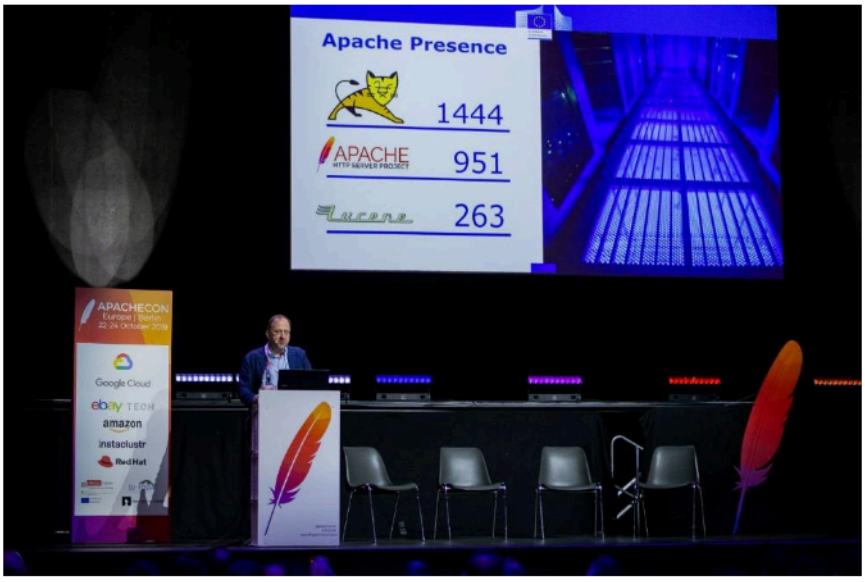

Figure: DIGIT Director and EU-FOSSA 2 Project Owner speaking at the ApacheCon Europe open source conference in Berlin, October 2019.

2.6.4. Impact on European Public Administrations

- Across the EU, public services in many member states (e.g. in France, Italy, Germany, Greece, the Netherlands, Belgium, Portugal, Estonia, Sweden, Denmark, to name a few) have become aware of the EU-FOSSA 2 initiative. The project has benefited significantly from the energised discussion on their experiences, role and responsibilities in open source.

2.6.5. Impact on the General Public

- EU-FOSSA put a spotlight on open source tools
- Focus on security has increased
- Massive response from open source software developers
- The general public is now more aware of the concept of open source. Whilst it is not yet a mainstream topic, the project generated great interest via the public survey.

2.7. Key observations from open source events

1. Islands/pools of open source solutions/excellence
   - The different pace of adoption and usage of open source has created a number of pools/islands of open source solutions/excellence across parts of Europe.
   - Rising interest in open source and a lack of awareness of existing open source ***solutions*** already developed in other parts of Europe *means a significant amount of rebuilding of the same or highly similar open source solutions*, or the purchase of proprietary systems. This leads to wasted finances, time and opportunity.
2. Security and resilience
   - As European Public Services embrace more digital solutions, increased and more sophisticated cyber-attacks on all systems, are inevitable.
   - It is imperative to ensure the most critical open source used across European Public Services is resilient and protected from such attacks.
3. Sustaining core open source (technologies and skillsets/people)
   - There is a set of open source software, which underpins the wider open source systems/solutions running across European Public Services. We need to sustain ***both*** the software itself ***and the*** development communities to maintain these core open source software.
4. Supporting small developers to keep innovation alive
   - Due to increased interest in open source by large private companies, we have increased polarisation within the open source world. Some large communities are well funded, whereas the smaller ones often struggle.
   - There is a need to encourage, fund and sustain the smaller developers, who currently struggle to fund themselves in innovating new open source projects or contributing to existing projects.
5. Diversity
   - Open source development communities can significantly improve diversity by attracting more women and BAME communities. As organic diversification will take a long time, there is room for some proactive measures to stimulate diversity.

6. Engaging SMEs
    - SMEs are under-represented in open source projects of European Public Services, and continue to seek increased participation. Suggested solutions include change in procurement practices and legislation to guarantee a certain percentage of revenue.
7. Encourage cross project sharing/re-use of standards/practices
    - There is wide body of best practices across open source projects. Due to various reasons including a lack of time, the disparate location of such knowledge, these is an insufficient sharing and reuse of these best practices. This leads to inefficiencies and reinvention.
8. IT Support
    - Both large and small European Public Services need IT support for mission critical systems they aim to build with open source. Technical project knowledge often lies with the smaller software communities, who are not able to provide such support scale; and the larger IT establishments often do not have the technical expertise.

3. PREPARATION AND OSS STUDIES (WP1)

This section makes some key observations and outlines the high-level lessons learned for work package 1.

3.1. Project charter (D1.1)

Creating the Project Charter
• The project charter was crafted during Q1-Q2 2018, at which time the bug bounty call for tender, was still in process. • In the kick-off project steering committee meeting, the MEPs directed the project to address wider issues surrounding Cybersecurity and open source. This led to the inclusion of two specific studies – see D1.4 and D1.5 below.
Enduring Value
• The project charter defined the scope and direction of the project at the outset. As such, during points of debate relating to scope, it provided a very useful compass. • Looking back at the Project Charter at end of the project, we find that the initial thoughts on the project objectives, scope, success criteria and risks, remained valid and of value. • In areas of first-time effort e.g. bug-bounties, success criteria were not well defined, and this is due to the project's lack of knowledge. For instance the number of bugs reported which turned out to be real bugs accepted by the software community, was difficult to predict, and by setting the target at 50%, this proved unrealistic. We now know that industry benchmarks differ from 15%-35% based on whether the software being tested is front end, middleware or back-end, with the front end bugs being more accepted. This is due to the middle and backend software usually being more resilient if they are of software that has been in operation for some time. • Despite such experiences, the EU-FOSSA 2 project charter proved to be a well-written and useful document.

3.2. Bug bounties proof of concept (D1.2)

Running the bug bounty PoC
This was a short, 6-week bug bounty run by HackerOne of the US, on VLC software. Despite it running over Christmas 2017 and the New Year 2018, it proved effective. For the project, it validated that: • We can successfully run bug bounties • Bug bounties are highly cost effective (there was unspent bug bounty prize money) • 6 bugs were found within this short period (a great success cf. code-reviews)
Money management and currency issues
• Working with a US company, we were working in Euros and they in USD for their platform fee and as well as the bug bounty rewards. This caused some currency exchange issues. • Lesson 1 → It is best to pay bug bounty awards on invoice, and not to send the entire reward budget to the platform in advance. If this is not possible, the supplier should hold funds in a Euro account. • Lesson 2 → ensure currency issues are discussed and managed at the outset of projects • Lesson 3 → For the larger EU-FOSSA 2 project bug bounties, rewards were set in Euros and necessary terms have been added to the call for tenders / framework contracts.

Project Reporting
• The PoC helped both the supplier and DIGIT fine tune the format of the numerous progress reports.

3.3. Lessons learned from the EU-FOSSA pilot (D1.3)

The experience of delivering the EU-FOSSA pilot highlighted a number of key lessons for the preparatory action stage. These lessons can be seen on Joinup at:

https://Joinup.ec.europa.eu/solution/eu-fossa-pilot/document/project-deliveries

3.4. Support and IPR requirements for FOSS free and open source software usage within European Union institutions (D1.4)

Task: In the backdrop of increasing open source projects within the European Commission and institutions, open source projects will need guidance on (i) Intellectual Property Rights/Licences, and (ii) securing ongoing IT Support for the software they use and solutions they craft. The objective of this task was to *establish our requirements* for these two areas.

Data collection
• IPR and Licencing are complex topics and it was challenging to find the right people to contact. • Once found, a survey was sent, but proved ineffective, as the questions, though simplified, proved to be too generic, complex and unable to be answered well. • Therefore the project relied more on the face to face interviews that were setup.
Synchronisation with the supplier
• There was delay from the EU-FOSSA side in identifying the right people, getting the survey answered and interviews set up, not just due to the complexity mentioned above, but also due to a heavy workload from other work packages. • The project regained focus, when a few months later, a new PM was appointed and some of the project's other pressures had reduced. • It is also worth pointing out a lack of synchronicity between both sides in the process to be followed to arrive at the outcome. This was due to a difference in working styles.
Effort and Meaningful result
• Detailed guidance led to an improved understanding and additional focussed effort by the supplier, led to a successful completion of the task, and the production of meaningful output.
Key lessons
• Neither side had anticipated the complexity of the task, nor did this lead to unrealistic project milestone planning. • The pressure to meet these timeframes and a hesitancy to *continue to be difficult* meant that the survey questionnaire was not adequate. In future, greater attention should be paid to the user impact of such data collection methods and contingencies should be planned for a poor show of results. • Where possible, one should continue to resist agreeing to/signing off unsatisfactory work items just to "get on with it". • Equally, we need to ensure that companies better understand the work to be conducted instead of putting all steam on sending a good proposal, which then cannot be easily achieved.

3.5. Review of FOSS usage worldwide and input towards OSS policies of European Union institutions (D1.5)

Data collection
• Due to the high profile of the work package and its strategic importance (its output would influence DIGIT/European Commission's open source strategy amongst other things); a large number of people were interviewed and surveyed. Audiences included internal DIGIT and other EC DGs, the European Council, the European Parliament, external think tanks and influencers and private companies. • Recent and past studies on FOSS were referenced, going back 5-10 years.
Synchronisation with the supplier
• The team worked very well with the supplier and was able to guide and influence the progress of the study in a positive manner. • The supplier was able to put forward a subject matter expert who understood the task well. • Overall the assignment went relatively smoothly
Lessons
• A close working relationship and deep knowledge of the subject was necessary from both sides; else, it would make a poor buyer/supplier relationship, and the output would have been voluminous, but rather less meaningful than it has been. Because of this tight cooperation, we have an excellent study and now an even better understanding of the state of open source software worldwide, with special regard to its use within public administrations.

3.6. Common observation on the FOSS projects

The lack of Open source knowledge
"Nothing can be loved or hated unless it is first understood." Leonardo Da Vinci. • Just like the rest of the European institution staff themselves, it would be fair to say that most of the current consulting organisations with framework contracts to provide consulting services to the Commission, also lack uniform knowledge and expertise in open source. • However, on assignments specific to open source, this lack of awareness can cause significant hindrance to progress. The project team is not expected to explain the very definition of open source. Examples include mistaking open source software for unlicensed software, being completely new to the debates involving open source, having little experience with common open source applications, and open source software development tool chains, and a superficial understanding of the subtle yet crucial role of open standards. • Consultants that do not wholly understand or appreciate open source will make odd impressions on expert Commission officials and involved member state representatives who they contact about open source at the Commission. This reflects negatively on the European Commission. • Consultants who use solely proprietary technology while working on strategic advice on open source, are unknowingly, meta-communicating a disregard for the topic to open source aficionados.
Using sub-contracted open source experts
• For the two specific contracts for studies on this topic, both consultancies recognised this gap early on, and remedied it by bringing in *third-party open source experts* as part of their team. • However, this approach brings with it its own share of problems. For one, in the guise of a unified team, there are really two teams - the expert/s who know/s and others who only know the consulting process.

- Further, the FOSS expert is limited by time constraints imposed by the consulting company.
- In our experience, this led to a considerable increase in effort by either the Commission or the open source expert bringing the rest of the team up to speed on open source matters.
- Often, the project team had to communicate open source related ideas and concepts to the regular team, who then had to pass the information onto the expert.
- This hindered the effective transfer of information and knowledge, and added risks to the outcome of the project.
- Please note that, with considerable efforts on all sides to overcome these handicaps, both studies led to acceptable results.

Lessons learned

- One way to help overcome this barrier could be to require consultancies in the framework contract to demonstrate *long-term practical involvement of open source staff/experts*.

4. EXTEND INVENTORIES (WP2)

This section deals with the lessons learned from the FOSS inventory update for the European Commission and its extension into other European institutions.

The project extended its offer to carry out a FOSS inventory to the following European institutions: European Parliament, Council of Europe, Council of the European Union, European External Action Service, European Economic and Social Committee and Committee of the Regions and the European Investment Bank. Of these, the European Council accepted. It is worth noting:

- Each institution is, naturally, at a different stage of FOSS usage and maturity
- Overall, every institution we spoke with, was enthusiastic about open source and its use within their organisation
- Some institutions felt they were too small for such a methodical exercise to be conducted
- Some institutions said that the timing was not right at the moment

4.1. Improved inventory collection methodology (D2.1)

Data collection
• Taking into account the lessons learned from the earlier inventory exercise conducted within the EU-FOSSA Pilot, the EU-FOSSA 2 inventory took into account a wider data set. • The current inventory collection methodology proved fit for purpose, and therefore did not need to be changed. In a way, it validated its suitability and usefulness. • The methodology is being used for the FOSS inventory exercise at the European Council.

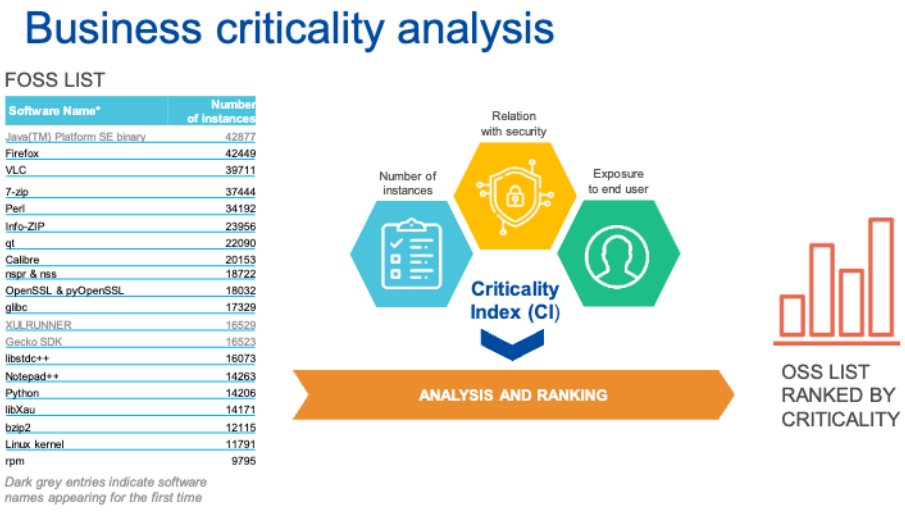

Figure: The methodology used to arrive at critical OSS.

4.2. Inventory of free and open source software used at the European Commission (D2.2a)

Larger Data Set → Improved inventory
• The larger dataset used resulted in results that were quite different from the previous inventory. • This led to a detailed examination (and re-examination) of the entire inventory methodology and the processes applied to arrive at the results. After an exhaustive analysis, and some corrections, the results of the current inventory exercise were accepted.
Inclusion of planned open source software
• We had wanted to include a list of planned to open source software in this updated inventory. However, the project was not able to obtain this information by system extracts, and so we asked via emails. Sadly, the response was poor, and so the exercise was not adequately completed.
Inclusion of current and planned open source projects
• The inventory was also to include *planned* open source projects, and those *currently in development*. However, the project was not able to obtain this information by system extracts. A manual exercise provided poor results, and the exercise was not adequately completed. • The lesson here is to assess at the outset (in the project charter) whether such information is *nice-to-have*, or *essential*. Based on that, the information collection exercise could be launched in the early stages of the project. In this case, the project decided that such information was indeed *nice-to-have* and the additional effort needed to accurately collect this information, could not be justified.

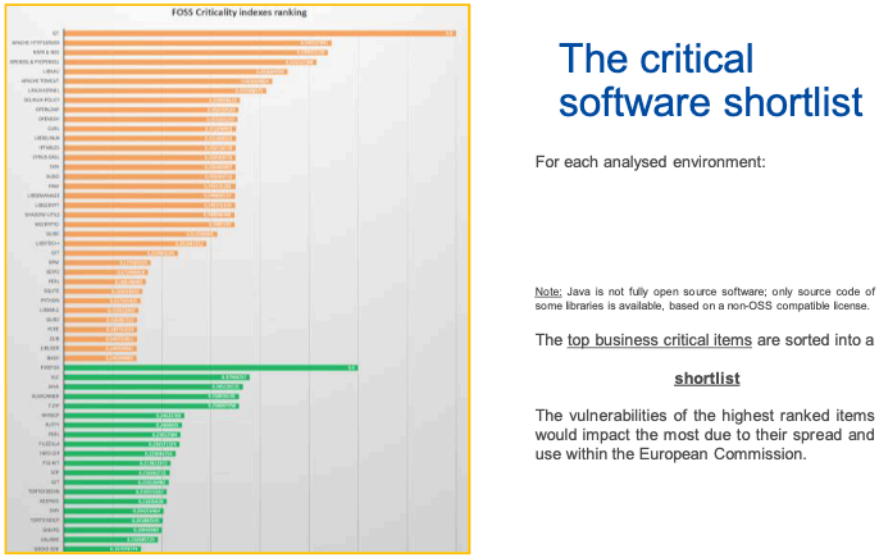

Figure: The final critical OSS shortlist

4.3. Inventory of free and open source software used at the European Council (D2.2b)

Observations
• The European Council's take up of the EU-FOSSA project's offer to conduct an inventory collation and analysis of their FOSS, was a welcome and encouraging sign of the uptake of open source at the European Council.
• As this was the first time, data extraction from Council's systems took a long period of time.

4.4. Rationale and list of software to be audited (D2.3)

This rationale is documented and is available on Joinup at https://Joinup.ec.europa.eu/solution/eu-fossa-pilot/document/project-deliveries.

Lessons learned
• It is difficult to predict in advance which software will benefit most from a bug bounty treatment. Typically, software with front-end interaction will yield more bugs, and middle/back-end server software will yield less. This was borne out in the bug bounties. Therefore, a judgement is needed as to the selection of software. • Further, it is important to not waste precious bug bounty money on software that has recently been subjected to a bug bounty programme by another customer, worldwide. Alternatively, to invest in a software which is under constant security monitoring by a well-funded parent organisation e.g. FireFox from the Mozilla Foundation. • Lastly, to make the selection more inclusive, the desires of the participating institutions and public were taken into account.

4.5. Publication of inventories (D2.4)

Publication of the European Council Inventory
• This is a decision on the part of the European Council towards the end of the project in Q3 2020.

5. BUG BOUNTY FRAMEWORK CONTRACT (WP X)

We called this work package X, as it fell outside the execution phase of the EU-FOSSA 2 project. WP X referred to the procurement/tender exercise to appoint the bounty platform providers, and so was on a critical path for the Project.

Elapsed time
• The first conclusion is that we managed to receive offers from the right candidates (SMEs and specialised companies active in OSS), and were able to grant the contract to companies that have implemented them efficiently. This means that the tender specifications were well drafted and more importantly, that DIGIT B3 did an excellent job in analysing the market and the needs of the Commission.
Elapsed time
• The process took a very long time and bug bounty providers were appointed in Q4 2018 as opposed to Q3. This delay impacted the project, but the delay was managed by the team.
Limitations placed by the structure of the contract
• Each bug bounty was a *separate standalone contract*, and so the team or the bug bounty platform could not allocate/use finances ***across*** bug bounties. This meant the project team had to predict the financial allocation before the testing started without knowing the precise state of its security robustness. • During the bug bounty process the project realised that the way the European Commission structured the platform fee in 2-month periods of engagement, *is not the usual way bug bounties are structured*, which are often engaged for the entire period, e.g. one year.
Lessons learned/Future actions
• This was the first time the financial regulation of the EU institutions, designed for predictable and established needs[9], was successfully married with a matter as unpredictable as the bug bounties. Source: DIGIT Procurement • Consider mechanisms for bug bounties to share a common budget • Consider different ways to engage bug bounty providers in their platform fees • Find out more about how others in the industry structure their contracts • Administrative burdens should be eased in order to increase participation but also to facilitate better performance. As an example, budgetary constraints forced us to come up with strategies in order to extend the duration of the specific contracts as much as possible but this also increased the administrative burden for our financial teams and the tenderers. Should those constraints be lifted, a simpler system of specific contract should be put into place. • Regarding IPR, in retrospect, we should reflect more on the ownership of the "results" (the bugs found), as the commission is not the "owner" of the OSS that are put into the system.

[9] Which often have a fixed budget.

6. SECURITY AUDIT (WP3)

The EU-FOSSA 2 project's primary aim was to make the OSS used by the European Commission and institutions safer. This meant *finding* and if possible, *fixing* security and other software vulnerabilities. The following four initiatives helped to achieve this outcome:

1. Bug bounties (find and fix bugs)
2. Hackathons (find and fix bugs)
3. Additional approaches – known bugs (fix bugs)
4. Additional approaches - architectural improvements (avoid bugs)

Note: Using the experience of the EU-FOSSA Pilot, the project team and the project steering committee decided to avoid code-reviews, as it was seen as being not as effective as the other available approaches.

6.1. Bug bounties (D3.1)

The project sanctioned 15 bug-bounties, all of which ran successfully.

1. 7-zip
2. FileZilla
3. KeePass
4. VLC
5. Notepad++
6. Drupal
7. PHP Symfony
8. Apache Kafka
9. Glibc
10. Apache Tomcat
11. PuTTY
12. Midpoint
13. WSO2
14. DSS
15. Flux TL

6.2. Bug bounty Summary Results (D3.1)

The bug bounty tender was won by 3 organisations. First was a consortium of Intigriti and Deloitte. The second was the company HackerOne Inc. The third was a consortium of two companies – econocom and yeswehack. Bug bounties were offered in a cascade, in the order mentioned here.

	Intigriti/ Deloitte	**HackerOne**	**econocom/ yeswehack**	**Total**
Total Bugs Reported	249	384	0	633
Total Bugs Accepted	57	138	0	195
Final Accepted Critical/High bugs	16	10	0	26
Total bounty rewards paid	€111,470	€89,400	0	€200,870

Note: Please see document D3.4 Bug Bounty Summary Report on Joinup
https://Joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliverables

6.3. Intigriti/Deloitte suggested Lessons

Contract
• The current setup where the service fee budget is shared with bounty budget is not convenient. It does not guarantee a constant budget available for vulnerabilities and all stats need to be updated frequently. It would be more interesting to have two budget lines, one for service fees and one for bounty+ bounty fees shared across projects, i.e. the entire bug bounty programme. •
Live hacking event
• An additional budget for a live hacking event would have been beneficial for more difficult applications. This budget pool would need to be quite large and finding researchers would be quite challenging, nevertheless the results could be very interesting as well.
Bonus
• To receive a possible bonus, a researcher should commit a pull request that can be accepted by the community as is, or the bonus would not be applicable. The bonus part is very interesting, but the validation process should be clear. The community should adopt the solution directly.
Community
• We are heavily depending on the goodwill of the community, especially to validate the submissions and fixes so we can ensure that they are not known duplicates. Most communities have their own direct line to report vulnerabilities and we have no visibility on these to see if the once we receive are new or duplicate. • Communication with communities is a challenge due to the fact that they are not the one who requested this initiative. In our opinion a stronger selection should be made. E.g. an initiative where companies can be a candidate for these types of exercises so their commitment is higher.
Type of applications
• The type of applications that are participating have to be a good match with bug bounty. Typically, finding vulnerabilities on libraries etc. have a low attraction grade (in any community), the same goes for specific protocols, etc. It is more interesting to ask researchers to test full applications (fat client. web application or mobile apps) where they can be creative to find vulnerabilities.

6.4. Code reviews (D3.2 – cancelled)

Due to the success of the bug bounties and hackathons, it was decided not to conduct any code reviews. In the EU-FOSSA 2 project charter, it was agreed that code reviews would only be conducted as a last resort, after bug bounties and hackathons and other initiatives e.g. the funding to Drupal.

6.5. Hackathons (D3.3)

In all three hackathons[10] (see Developer Engagement - section 7.4 below), software vulnerabilities were found, and fixed. The observations and lessons here relate only to the aspect of finding and fixing bugs.

Please see https://Joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliverables for the hackathon report - D3.2 Hackathon Summary Report. This is a comprehensive analysis of the hackathons.

Focussed working at one location ➔ led to tremendous productivity
• The EU-FOSSA 2 hackathons brought people together from all across Europe and some from further afield. Many had met face to face for the first time. • This presence of key actors, allowed many vulnerabilities to be solved quickly. • Further, new bugs were found and solved. • The PHP Symfony founder said that they managed to do over 2 months of work in 1.5-2 days!

Figure: At the end of a successful Hackathon

[10] See WP4 communication plan for further information on the hackathons.

6.6. Drupal security improvements (D3.4)

The EC being a heavy user of Drupal, decided to fund some pending Drupal security work.

1. Improve the *software vulnerability patch management process*, by **automating** it
    a. Study the system and arrive at a plan to implement
    b. Create the solution and implement it
2. Fix a number of already known security bugs

Please refer to the Drupal website for the work specifications and results achieved.

Cooperation creates safer code
• The EU-FOSSA 2 project sponsored the effort and Acquia[11] and the Drupal community developed the solutions. In the event, the project funding did not completely cover the costs of the automation, but provided the impetus for this long planned work. • This project went smoothly and all sponsored work is now complete. The new automated patch system makes for safer patch application in Drupal 7 & 8, benefitting not just the EC but also the wider Drupal user community. For more information, please visit GitHub and the Drupal site.

[11] Acquia is the professional services arm of Drupal.

7. EDUCATION AND OUTREACH (WP4)

7.1. Overview

The purpose of this work package was to support all EU-FOSSA 2 communication activities and in doing so, strengthen the level of engagement with stakeholders and open source communities, and continue to raise awareness of the importance of open source, its security and security in general.

Communication Plan
• A multi-channel communication plan was created to meet the core aims of the project. Overall, WP4 met its core objectives and the success criteria (defined at the project charter stage), and can be regarded as being highly successful.
Dedicated communications expert
• One of the key reasons for the success of WP4 is because the project was able to rely on a dedicated communications expert, who liaised with external suppliers to get the work done.
Key Lessons
• Given the amount of work in WP4, it was essential to have a dedicated person to manage the plan, communication activities and external communication and events suppliers. • Having **separate suppliers** for *communication* and *events* proved decisive to the success of each. This separation allowed us to hire specialists in their field.
Press clippings
• Whenever a project has an external outreach campaign that has an impact on media, it should have a clipping service associated to track all the mentions (press and online media). • For this task we relied on the goodwill of many journalists to send us the news after publishing, on google alerts, and on our communication supplier to spot any news.

7.2. The communication plan (D4.1)

The communication plan included the following key elements:

Improved the branding/visual identity	A dedicated project website
Public surveys	An outreach campaign
Engagement with developers	Ask Me Anything sessions on reddit
FOSS Leadership Conference	

Figure: Key components of the communication plan

7.3. Website

Usually DG COMM is hesitant to allow the creation of project specific websites. However, in the case of EU-FOSSA 2 they made an exception allowing a specific URL https://ec.europa.eu/eu-fossa2. This is in addition to the project's presence on Joinup at https://Joinup.ec.europa.eu/collection/eu-fossa-2.

7.4. Branding

To obtain greater impact than that of the EU-FOSSA pilot stage, it was decided to create fresh branding. A new logo and design guidelines resulted in a strong and coherent image. This allowed a higher level of outreach, engagement, and immediate recognition from the targeted audience. The following deliverables were executed to support the outreach campaign and other communication activities:

Logo rebranding and Visual Identity
• Usually projects do not have their own logo/visual identity; however, the EU-FOSSA pilot programme already had a logo. This was refreshed for EU-FOSSA 2 and proved a key component of the new visual identity.
Branded Merchandising
• To complement the events hosted by the EU-FOSSA 2 project, several branded merchandising items were produced, including: t-shirts, tote bags, stickers, pens, mugs and 3D printed phone stands.
Key Lessons
• A project with an external outreach needs to have a carefully planned communication plan. • It is useful to have a dedicated person to manage internal DIGIT/European Commission communication as well as external communication.

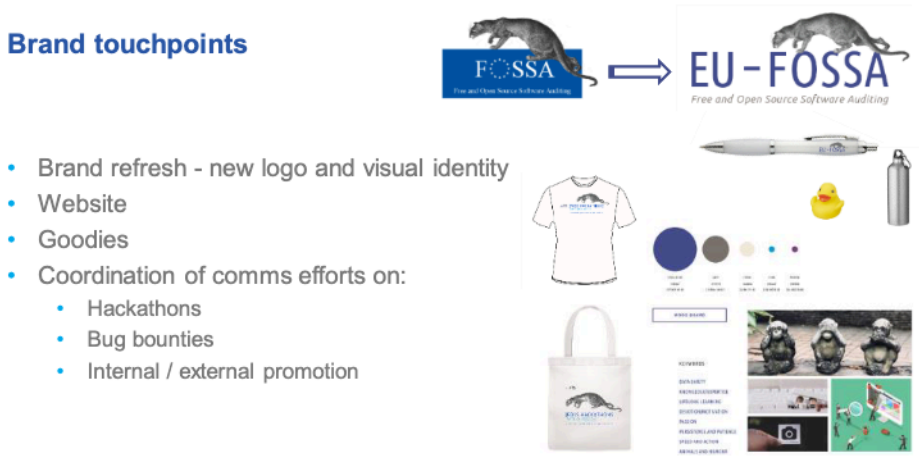

Figure: Re-branding touchpoints

7.5. Outreach Campaign

The outreach campaign aimed to raise awareness among the General Public, Free Open Source Software (FOSS) developers, and internal European institutional audiences about the benefits and challenges of FOSS, with a specific focus on **Security**. The campaign contained three main actions (i) Production of Communication Materials, (ii) Public Relations actions with multipliers and (iii) media relations, and paid social media.

Communication Materials Production
To support the outreach campaign, PR and engagement actions, the external communication supplier produced a set of materials, managed by the project's communication expert. • **Communication Materials**: The project produced the following materials: a poster, a generic presentation, an animated social media video, 3 Hackathon videos, rollups, an infographic, several articles and a project manifesto document. • **Press kit**: A press kit comprising the EU-FOSSA 2 Visual Identity; an EU-FOSSA 2 presentation; project manifesto, project poster and EU-FOSSA 2 Pictures (team, hackathons, AMA).
Multipliers and Media Relations
• In order to engage with the multiple audiences, the project created audience personas, identified their preferred communication channels, established relevant media contacts, open source journalists, and open source influencers (multipliers).
Paid social media
• Considering the targeted audiences, the project decided that paid social media would not yield much benefit. Instead, social media interactions focussed on the use of DIGIT's twitter account and the Joinup platform. This may have affected the dissemination of public surveys, PR actions with multipliers and media covered the lack of paid advertising. • In the end, this decision proved to be fruitful, and as a result, the number followers of DIGIT's twitter account increased as well as the number of subscribers of DIGIT's internal newsletter Be.Digital, and the surveys reached the right audiences leading to healthy survey participation.
Synchronisation with the Communication supplier
• The external communication organisation played a critical role, in the definition of each target

and supporting all PR actions. The synchronisation was smooth and effective, even though at times the supplier did not show the right attention to detail, requiring several revisions for each activity. This was particularly evident when it came to the subject of open source.
Effort and Meaningful result
• This meant unforeseen additional effort from the EU-FOSSA team side to review deliverables more than planned.
Key Lessons
• Communication materials were crucial to engage with the open source community and raise awareness about the importance of the security of open source. • PR actions not only supported the engagement with developers and the dissemination of the public surveys, but also compensated for the lack of paid social media actions. • Even though every supplier has a high level of attention to detail, there is always a need to review every deliverable provide more inputs "from an open source point of view"

7.6. Public engagement surveys (D4.2)

Public surveys

Two public surveys were conducted – one for *open source users* (the general public) and one for *open source creators* (the open source developer community). They were disseminated using social media, general and specialised media and multipliers through PR actions and direct contact. The engagement support of an external communication supplier was essential for the overall success of both surveys.

Public surveys
The purpose of the public surveys was to help the EU-FOSSSA 2 team to understand the level of aware of open source within the user community. Outputs from these surveys helped refine interaction with media and influencers. Overall, the key objectives of these actions were met, with the second survey (developers) commanding a high response rate. Therefore, we can conclude that PR actions targeting specialised media and direct contact with influencers, is highly effective when engaging with the open source community.
Public survey 1 – What does FOSS stand for?
• The first survey was launched in May 2019 in a quiz format, targeting general public. The quiz reached 321 individuals; the most successful channels were the media and the Joinup and DIGIT tweeter. Over half of the respondents mentioned knowing more about FOSS after taking the quiz.
Public survey 2 – Want to contribute to open source security?
• The second survey was launched September 2019 on EU survey platform, targeting open source internal stakeholders, developers and users. The survey reached 3184 individuals, a result of the specialised media dissemination along with Joinup and DIGIT tweeter.
Effort and Meaningful result
• There was a great amount of effort invested in this activity, not only to make sure the right questions were asked but also to disseminate both surveys to reach the target audience. As a result, 3505 people participated in both surveys and several articles came out on specialized media.
Key Lessons

- Using public surveys as a way to engage with the open source community, not only to collect their opinion but also as a way to disseminate the latest information proved to be a useful mechanism.
- The communication supplier must have someone who with deep understanding about open source to support its team.

Deliverables

Survey 1

- Raw data file
- Quiz report

Survey 2

- Raw data file
- Survey report
- Infographic

7.7. Developer engagement (D4.3)

A key remit of the project was to engage with the open source community and start a two-way conversation. To achieve this, the EU-FOSSA 2 team adopted a number of measures: conducting hackathons; participating in open source conferences; contacting micro/small open source communities directly; hosting a dedicated European open source conference for key open source leaders/stakeholders; and holding an AMA (ask me anything) session on reddit.

These actions proved fruitful and contributed significantly to the high level of engagement with open source developers and their communities.

Hackathons → (click to see the videos: First Second Third)
During the last year of the project, EU-FOSSA 2 held three hackathons, the first was dedicated to symphony community, the second was dedicated to the Apache community and the third and last one was dedicated to the EC Projects. An external event supplier BeMyApp, and the external communication supplier GOPA com., both managed by the communication expert, supported the organisation of all three hackathons. Overall, all three hackathons were considered highly successful in terms of attendance and results, but the last one proved to be the most successful one, due to high attendance levels and diversity of projects from the EC. It was the first time that the EC held an internal hackathon and exposed source code with developers form all over the world.
Existing Developer's events
• To disseminate EU-FOSSA achievements and the support of the European Commission towards the open source community, the EU-FOSSA team participated in several open source events with speeches and keynote presentations.
New communities engagement
• See section 7.8 below.
AMA session
• In order to extend the engagement with FOSS communities, EU-FOSSA team held an AMA (ask me anything) session on reddit. This was the first time that an EC project ever hosted a session on an external platform as reddit.

- The session was hosted by the EU-FOSSA 2 project and programme managers, an Open Source expert and the Project Business Manager. The audience was quite small, nine people, but the questions were pertinent, and the session was well regarded.

Comments by our communication partner on the AMA session:

- Despite being new to everyone, the AMA session on Reddit was a great success. After some initial problems getting in touch with the Reddit moderators, the session itself went smoothly and allowed the team to engage with the public, answer their questions, and present itself in a highly accessible way.
- The various pillars of the project could have been more integrated, for example the engagement sessions, the bug bounties and the hackathons, all revolving around developers.
- Dedicated channels like Twitter and other social media would have allowed reaching a wider audience, keeping in touch, and pushing out the content and communications. A presence on or a collaboration with platforms like StackOverflow could have also been beneficial for the project.

Foss Leaders Event - Open Source Beyond 2020

- The Open Source Beyond 2020 – Powering a Digital Europe was co-hosted with DG CONNECT. For the first time, the European Commission discussed open source software and hardware with FOSS leaders from all over Europe, addressed open source software and hardware in Europe. The event had two plenary sessions, and several parallel sessions to discuss different topics. All sessions were summarised by a rapporteur, which resulted in an extended report of the whole event. All and communication materials were provided by the external communication supplier, and the event was by teams from both DG's.

Key Lessons

- Physical hackathons are crucial and fruitful events, and should become a common practice for EC open source projects to meet the wider developer community and also to share ideas.
- The EU-FOSSA 2 project showed the open source community that the European institutions were doing something for the communities directly, and that the EU is not just a user of open source, but also a contributor.
- All efforts invested to engage with open source communities are a contribution to the increased adoption of open source within the European community.
- The communication supplier must involve an open source expert on a regular basis to discuss and review all materials produced before presenting it to the client.

EXTERNAL COMMUNICATION PARTNERS

GOPA COM. was the key communication partner.	**NOVACOMM** provided communication resource.
BeMyApp - Hackathons partner	**Brindiberica.pt** – hackathon merchandise supplier
Imprima3D.pt – small Portuguese company provided 3D printed foldable/portable phone stands.	

7.8. Engagement with small/micro communities

One of the harsh realities of open source is that many micro and small open source communities struggle to survive, let alone grow. Their challenges include all their resources working purely on a voluntary basis, a lack of funding and a lack of IT/ other resources.

The EU-FOSSA 2 team connected with a handful of such communities to understand their issues and assess how the EC can contribute to their success. The project team spoke with six communities via video conference calls - Toybox, OSHW/FPGA, Arduino, /e/, OKC/Autocrypt and LineageOS.

This section 7.8 states observations made by the open source expert who assisted in finding these communities and arranging the sessions. Though the observations do not belong to the project team, we find them astute enough to be included in this document for future consideration by open source stakeholders.

7.8.1. The sessions

- The European Commission reaching out was highly appreciated by the open source communities.
- Community members were very open to interaction and very transparent about their activities/ business/ needs.
- Quite a few of them, however, when asked for their needs, seemed to have problems articulating their non-technical, mid-long term needs, as if it was the first time someone asked them about it and they had never given this any thought before.
- Some of the developers/communities approached took more than four weeks to come back with their first reply, despite sending reminders through various channels. In the end, all approached developers/communities responded positively, except for one open-source hardware developer who was very disappointed in his earlier experiences in procuring EC funding.
- Some of the developers wanted a separate, more informal call before the official call with the EU-FOSSA 2 team, to explain what they were currently working on, to get a better feel of what was expected from them, or because they didn't want to be in a call with (specific) others.
- Issues discussed
- Despite sustainability being an important topic in the discussions, money/funding was rarely identified as a primary need. There also seemed to be some embarrassment to discuss funding openly. Time (to develop, to do more, better, faster) appeared to be the most wanted resource.
- Writing or contributing to open-source software is mostly done for free, mainly because to many of the developers, open source is a creative outlet. This focus on creativity (or enjoyment in creative-coding) means that a lot of other things needed to make code open source software into a usable final package (e.g. usability, security, documentation, packaging) are lacking, simply because these tasks are far less rewarding with regard to (personal) creativity and meritocratic appreciation by the community.
- Several developers admitted that their daytime job was only a way to be able to do (i.e. finance, subsidise) what they were most passionate about: working on their open-source projects. It would be interesting to find out whether subsidising some/part of their efforts

creates more (social/economic) value in a wider perspective in the longer term than their current "business model".

- It was clear that for some developers building a large user base appeared not to be a primary goal. Instead, their primary concern was often the developer community itself, and they appear to be incentivised by other (intrinsic) motives rather than financial reward. For this group, it is doubtful if financial rewards would help them. However, others did wish to grow their communities and would benefit by a cash injection.
- Interestingly, despite their main interest lying with the developer community, some (lead) developers appear to be very concerned with the integrity of their productions. Reproducible builds were a returning topic in the engagement conversations as well as during the open source conference in November.

- Some of them said that other governments were very explicit in inviting them over to work and start businesses in their countries. China, Japan and Singapore were the countries mentioned here.

7.8.2. High-level conclusions from the sessions

- A first conclusion would be that participating in open-source developer and user communities is useful and a necessity, since the public sector are developers and users of that very software themselves.
- However, since the general public are also users of open-source software, governments have a role to play in protecting and facilitating general public's usage, e.g. when it comes to security and interoperability (i.e. open-source software (and open standards) as a commons).
- Furthermore, creating and using open-source software and hardware (e.g. the European Processor Initiative (EPI), the EuroHPC Joint Undertaking, and RISC-V) has been identified as a way to differentiate the European Union from other economic powers, just like open data and open science/access, and the European culture of openness in general. This extends the importance of the "open movement" further to include the private sector as well, for example in open design and co-creation.
- Rather than trying to "convert software developers into entrepreneurs", a facilitating and complementary approach may prove to be the better way to accomplish the European Commission's goals. This includes the security and integrity of the software, but also sustainability, usability, services and other facilities that turn open-source software into a healthy (i.e. future-proof), deployable product.
- The way open-source is organised lends itself naturally to such a complementary approach: the licenses allow you to use and extend the software in various ways. For example, fixes, additions and improvements can be contributed upstream in the form of patches. The same is true for all sorts of documentation and training materials. Or existing code can be built upon and be published (downstream) as software, a package or a product (i.e. building up a product/value stack).
- With regard to the latter, open-source software businesses typically build on a service model (e.g. Nextcloud), or the (somewhat controversial) open-core model, rather than the classic product software business model ("write once, sell many copies"). It has been suggested that the value component that cannot be monetised (because of the open-source part underlying the value proposition) hinders open-source businesses in growing fast and large enough to become sustainable/competitive. That needs further looking into, as maintenance, troubleshooting, support, training, etc. are pivotal in turning open-source software into a deployable product.

- Some developers have mentioned that using a free software license instead of a (permissive) open-source software license in practice does not help you in protecting your productions and keep companies from using your software in their commercial products without adhering to the license terms. According to them, some large companies will counter their complaints and claims, draining their scarce time and resources. The developers' lack of market and legal strength was mentioned a couple of times as one of the points where the European Commission could provide help with.
- Another thing mentioned by several developer groups was that they had a need to get together to solve specific problems or get specific development initiatives started, but lacked the resources to do so themselves. The European Commission could help these communities by facilitating hackathons to bring together developers working (remote) on the same project, like they already did for some other developer groups as part of this project e.g. at the Hackathons.

7.8.3. A multi-faceted, complementary approach to open source development, deployment and business

- As open-source communities will generally not produce (for free) the full product/value stack that is needed to turn their code into a secure, deployable software product, a multi-faceted, complementary approach may be the best way for the European Commission to fulfill its own needs and what it thinks is important to others (i.e. the broader private sector, the general public, and the private sector, as discussed above). Multi-faceted, because this involves different elements along the product/value stack (e.g. documentation, audits and packaging), but also market opportunities for a service-driven business model, and the legal power to protect the rights of developers. Complementary, because trying to (financially) steer developers into a different direction or lure them into producing something they are not passionate about, may very well have an opposite effect.
- The conclusions above show that there are specific needs open-source developer communities have, providing plenty of opportunity for the European Commission to help the community, thereby helping itself and other public organisations as a user, as well as the general public and even the private sector.
- As discussed above, in most cases, the full range of requirements that make software into a mature, usable product/value proposition is unlikely to be met by the small/micro open-source community as it is. Simply contributing to or funding the functionality that the European Commission is using/needing itself and that they think/see is important to the general public, will generally not be enough to solve the problems they are addressing in this project, i.e. the security and integrity of the open-source software that they and the wider public is using. Rather than trying to change the developer community into catering to its needs, the European Commission could be facilitating and be part of the process that turns the high-value work done by the open-source community into usable packages, products, services and propositions.
- A multi-faceted approach along the whole value chain from raw source code to a complete product/value proposition seems appropriate:
    - The creative part of open-source software development can be facilitated in the same way as other creative sectors are funded.

    - This creative output can be turned into a complete/mature product by funding (maybe even in a targeted way) the complementary parts that are not and will not be created by the community for free, simply because it's work rather than creation.
    - The start-up and growth of businesses providing the services required to turn a software product into a complete, deployable, competitive value proposition should be facilitated.

- There is an incredible amount of value created and freely available as open source. The European Commission could develop criteria specifying what type of projects could receive what type of help. On the one hand, a programme could be set up allowing individual projects to apply for help with their specific needs. On the other hand, for project that they have a special interest in, the European Commission could for each individual project identify/ask where along its value stack/chain the needs and opportunities are where they could hook up to help move these open-source productions up the stack. This selective approach would put the immense value of this open-source slush pile to better use in an effective way.
- The trick will be to nourish the creative source at the bottom of the stack without destroying it, while at the same time stimulating and facilitating (co-creating?) the much needed parts higher up the stack.
- A multi-faceted approach is already emerging from the direction the EU-FOSSA initiative has been developing: from security-focused, audits only, and direct needs the initiative expanded to hackathons, bug bounty programmes, engagement sessions and an AMA, addressing the needs of the EU institutions as well as those of other public organisations and the general public. At the same time the scope has widened from security to sustainability, as that may be a far more important aspect than security knowledge, the availability of best practices and mentors – to name a few – to increase security and integrity.
- The EC (or public agencies in general) should be aware of the dual role they play – i.e. the leverage they have – in the software market:
- They have both market power (as a large user and buyer of software) – think procurement requirements and preferences; and legislative power (as a market regulator) – think setting open standards and funding reference implementations.

8. POST EU-FOSSA2 (WP5)

8.1. Lessons Learned

A lessons learned document was produced – *this document*. The lessons learned are summarised in the project chapter above and distributed across each work package.

9. DISSEMINATION OF RESULTS (WP6)

9.1. Presentations

In addition to the events mentioned in WP4, the project team was able to interact with the open source community and public in the following open source events:

When	Event	Location
Feb 2018	Fosdem	Brussels
May 2018	SuperSEC, Spain	Almeria
Nov 2018	Linux Europe Open Source	Edinburgh
Dec 2018	Paris Open source summit	Paris
Feb 2019	Fosdem	Brussels
Oct 2019	ApacheCon Europe	Berlin
Nov 2019	Linux Europe Open Source	Lyon
Dec 2019	Paris Open source summit	Paris
Feb 2020	Fosdem	Brussels

Observations
• The presentations in 2018 explained to audiences what the EU-FOSSA programme was about, the ones in 2019 related more to the sharing of the results. • These events provided an opportunity to meet attendees from other organisation, public and private, open source practitioners, open source leaders, open source foundation leaders and open source legends such as Linus Torvalds. • Via these events, the project was able to share what the Commission and institutions was doing in the realm of open source and understand the state of affairs in other establishments. • A summary of these observations are included in the Project section (chapter 3) above.

9.2. FOSS leadership conference

A DG CNECT/DG DIGIT (i.e. EU-FOSSA 2) joint conference, **Open Source Beyond 2020**, *Powering a Digital Europe* was held on 14/15 November 2019. Please visit this page on Joinup https://Joinup.ec.europa.eu/collection/eu-fossa-2/news/open-source-beyond-2020-review and this page on EC Europa https://ec.europa.eu/digital-single-market/en/news/workshop-about-future-open-source-software-and-open-source-hardware.

At the event, conference participants and Commission staff debated the key challenges and opportunities within open source, discussed the sustainability of business models supporting open source communities, and the frontier of research and innovation in both open source software and open source hardware.

The event resulted in a variety of suggestions from *open source advocates* and *open source SMEs*. A summary for each panel can be found in a document uploaded onto Joinup - *EU-FOSSA 2 - Panel reports from the workshop on Open Source Beyond 2020.pdf*.

In addition, EU-FOSSA 2 is sending to DG Connect a summary of the project's key observations and findings about the state, issues and challenges faced by the European open source software ecosystem. Please see section 2.7 above for more information.

Open Source is critical to EU's Digital Growth
• Though it is difficult to summarise in a single paragraph, attendees requested the European Commission to do much more to promote and sustain open source in the European Union, using tailored procurement, creating new legal frameworks to increase SME participation, and a clear preference for or obligation to use open source.

10. PROJECT MANAGEMENT (WP7)

10.1. Project Manager

Project Manager
• A suitable external project manager joined the project in December 2017.
Lessons Learned
• It was very difficult to find a suitable project manager via existing framework contracts (see also the chapter on lack of expertise at the suppliers – see section 3.6 above). • There seems to be a rift between the "corporate world" and the "open source world", with people rarely moving across, making it very difficult to run a project like this one, focusing on OSS. Only using a different framework contract, with significantly higher daily rates, provided some suitable candidates with wider horizons, including the OSS.

10.2. Project Steering Committees (PSCs)

Senior Management Commitment and Support
• Over the course of the project there were five steering committee meetings held. There was tremendous support from the sponsoring MEPs, DIGIT senior management from Director General level, including presence in four of the five meetings. • The PSCs allowed for valuable directional input during the execution, allowing the project team to increase focus on specific areas. One of these was to "help *fix bugs*, not just *find* them"; another was to examine the wider open source ecosystem and learn about their issues, about security, working practices, challenges faced and sustainability. • In order to increase MEP or "business input" to the project, an MEP assistant was appointed as Business Manager to the project. This appointment proved critical the success of the project

11. CONTINUATION OUTLOOK

The EU-FOSSA programme, the Pilot and the preparatory action have now completed. The next step would have been to make the programme, a permanent standing activity.

In the coming years, the use of open source software within the European institutions and the EU in general, is likely to increase. At the same time, as the organisations mentioned embrace *digital* more and more, we are likely to see a corresponding increase in Cybersecurity threats, both for proprietary and open source software and solutions.

Therefore, the case for the core objectives of the EU-FOSSA programme, namely, ensuring the robustness, security and sustainability of open source software, is undisputed.

The only question is how we structure ourselves from an organisational and financial perspective, to meet these objectives. Therefore, it seems sensible to take some time and properly consider the response to these questions.

In this regard, the European Commission is taking the following concrete next steps:

1. Provide the key findings of EU-FOSSA programme to DG Connect ➔ for consideration for inclusion within the Digital Europe Programme (DEP).
2. Continue a subset of the EU-FOSSA 2 type of work under the ISA[2] programme ➔ a project has been approved[12] and will start in June 2020.
3. Support MEP Marcel Kolaja's proposal for a new pilot project to explore the question of sustainability of the European open source software ecosystem.

[12] Please see page 916 in the PDF accessible via the link shown here. This describes the scope of work https://ec.europa.eu/isa2/sites/isa/files/wp_2020_detailed_description_of_actions_part_2.pdf

12. LIST OF REFERENCES

[PilPr] "Pilot projects and preparatory actions in the annual EU budgetary procedure" http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/640130/EPRS_ATA(2019)640130_EN.pdf

[FinReg] EU Financial regulation https://ec.europa.eu/info/publications/financial-regulations_en

[PrCh] EU-FOSSA 2 Project Charter at https://Joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliveries