DG DIGIT
Unit B3

EU-FOSSA 2: Establishing high-level requirements for the provision of assistance in the areas of "IT Support" and "Intellectual Property Rights" to open source software projects at selected European institutions and an analysis of the market

D11.01 Final Report Public Version

EU-FOSSA 2: Contract ABC IV-000167 Lot 3, DI/07624

Date: 04/05/2020
Doc. Version: 1.2

This template is based on PM² v2.5

DOCUMENT CONTROL INFORMATION

Settings	Value
Document Title:	D11.01- Final Report Public Version
Project Title:	EU-FOSSA 2: Contract ABC IV-000167 Lot 3, DI/07624
Document Author:	Trasys International (part of the NRB Group)
Commission Project Managers (CPM) (European Commission) :	EU-FOSSA 2, OSPO (EU-FOSSA 2, Open Source Programme Office)
External Contractor Project Manager (ECPM):	Trasys International (part of the NRB Group)
Doc. Version:	1.2
Sensitivity:	Internal
Date:	04/05/2020

Revision History

Date	Version	Description	Author(s)	Reviewed by
09/03/2020	1.0	Initiation of the deliverable	Trasys International (part of the NRB Group)	OSPO (Open Source Programme Office)
28/04/2020	1.1	Modification of the deliverable following the Customer's observations	Trasys International (part of the NRB Group)	EU-FOSSA 2 Project
04/05/2020	1.2	Minor modifications	EU-FOSSA 2	EU-FOSSA 2 project

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this document. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

PM² PROJECT MANAGEMENT METHODOLOGY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

European institutions have *used* open source software for over 20 years. In recent years, the European Commission amongst others, has also become an active *contributor* of open source software and has created many open source solutions for public use, one example being EU Survey.

DG DIGIT, the European Commission Directorate General for Informatics is the largest IT function of the European institutions, and is leading the way open source is used and governed. Its open source strategy has been renewed (2019/2020) and paves the way for an increase in open source projects in the coming years.

This increase in open source software usage by projects will necessitate better governance of licencing and intellectual property rights (IPR). Further, the software and resultant solutions will both need on-going IT Support and maintenance.

This study has been commissioned by the EU-FOSSA 2 project, to establish the needs of current and future open source projects within the European institutions for support in two areas (i) IPR support and (ii) IT support. Further, the study conducts an analysis of the marketplace for best practices in open source users and solution providers in these two areas.

This study will lead the reader to the conclusions that a formal open source governance must be established and implemented by the organisation. Gartner[1] confirms that need to manage technical, security and legal risks in the context of open source projects: "*When unmanaged, these same OSS technologies will instead introduce considerable technical, security and legal risks to the enterprise*".

This study highlights the necessity for the European organisations adopting open source projects to manage those aspects in terms of software maintenance and licensing through activities grouped as follows:

1. Open source software Governance
2. External IT Supporting Management
3. Internal IT Supporting Management
4. Quality Management
5. Identification of a maturity model and identified targeted levels
6. Information and knowledge
7. Automated tools
8. Monitoring tools

The study's chief output is a set of requirements for IPR and IT support for the European institutions, presented in a manner that facilitates inclusion in a call for tender, at an appropriate time. Accompanying the requirements are a list of useful questions to further probe and refine each requirement.

[1] Gartner, "What Innovation Leaders Must Know About Open-Source Software", Arun Chandrasekaran, Mark Driver, 26 August 2019

1. INTRODUCTION

This document represents the final report of a Study that was requested by DIGIT in the context of the Preparatory Action Project "Governance and quality of software code – Auditing of free and open-source software (26 03 77 06)". The project in relation with this Study is labelled as the EU-FOSSA 2 Project, with FOSSA standing for Free and Open Source Software Auditing.

Trasys, which is part of the NRB Group, has been mandated for this Study by receiving the Technical Annex (ABC IV framework contract) relating to work package 1.4 of the larger EU-FOSSA 2 project, and by being selected for the proposal that has been submitted in response to the received Technical Annex.

The Technical Annex lists 11 Tasks, from 1 to 11, which refer to the following work description:

- Task 01 (PM): Overall project management, reporting and coordination
- Task 02 (Execution): Analyse and document the intellectual property support requirements of the European Institutions that are within the scope of the study
- Task 03 (Execution): Study the market for leaders and best practices in intellectual property management and deliver a comprehensive report
- Task 04 (Execution): Analyse findings and propose a way forward for intellectual property support that meets the needs of the European Institutions
- Task 05 (Execution): Prepare formal requirements for Intellectual Property Support requirements
- Task 06 (Execution): Analyse and document the software support and system support requirements of the European Institutions that are within the scope of the study
- Task 07 (Execution): Study the market for leaders and best practices in software and system support and deliver a comprehensive report providing a status of the current situation in terms of best practices
- Task 08 (Execution): Analyse findings and propose a way forward in terms of software & system support, that meet the needs of the European Institutions
- Task 09 (Execution): Prepare formal requirements for software system support requirements
- Task 10 (Execution): Prepare the final report
- Task 11 (Closure): Prepare a public version of the documentation

As set out in TASK-10 of the Technical Annex, this document includes content that has been produced through all previous project deliverables in relation to TASK-02 through to TASK-09; the main elements of which are summarised in the following sections of this final report.

The deliverables of TASK-02 and TASK-06 identify the intellectual property support requirements and the open source software support requirements of the European institutions. This was achieved using a questionnaire via the EU Survey online portal and through interviews. Both methods were aimed at internal teams known for using open source components. More specifically, the investigations have included a discussion around:

- the existing initiatives undertaken by the panel of interviewees and survey respondents;
- the level of maturity reached in the field of open source software components configuration;
- the ability to choose among different products or solutions taking into account the intellectual property constraints, as well as software management and software support needs constraints;

- the problems related to intellectual property, as well as software management and software support needs, faced while implementing new solutions;
- The expectations of the targeted audience towards concrete support and related procedures to be set in place to enhance communication with dedicated legal and IT experts.

The deliverables of TASK-03 and TASK-07 highlight the best practices and lessons learnt in intellectual property management for open source software and in open source software support management from external leaders, end-users and solution providers from the public and private sectors. For this purpose, a research activity was carried out: this has led to the collection of various documents and webinar transcripts. Furthermore, several interviews with open source leaders allowed to gather information about the way in which they manage open source software, both in terms of intellectual property rights management and support. The interviews covered items such as:

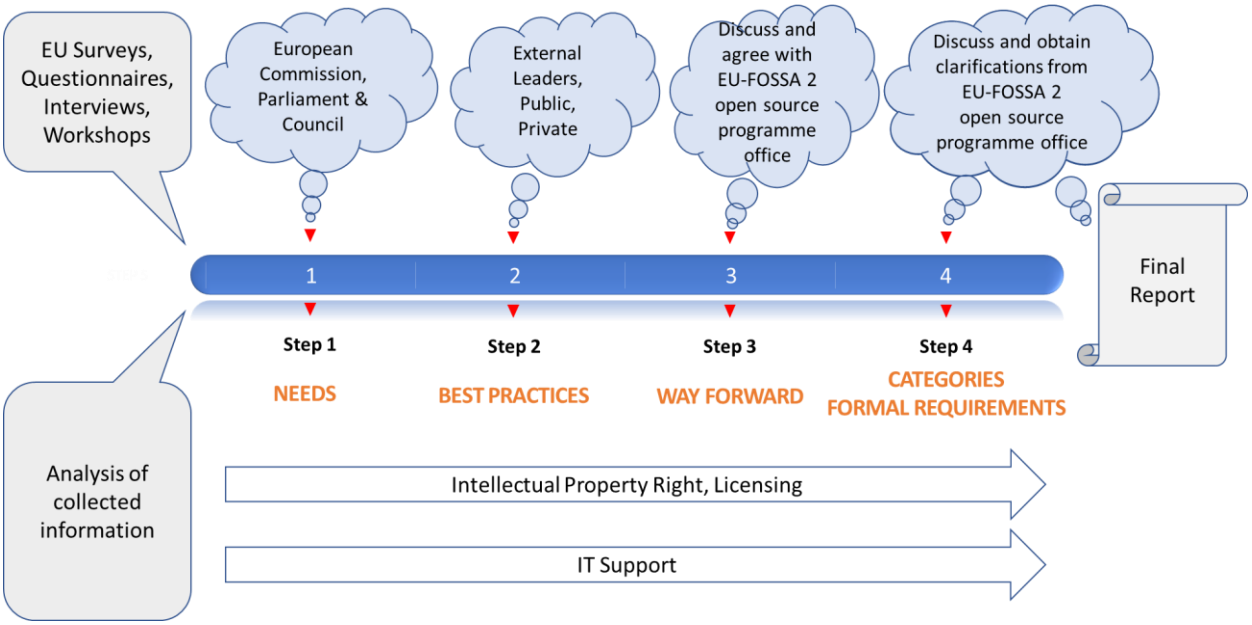
- innovative entities;
- developers;
- advisers;
- reference entities that promote open source software;
- advanced users;
- solution integrators;
- software publishers.

The deliverables of TASK-04 and TASK-08 suggest a way forward for both intellectual property rights management and support for open source software. More specifically, they include a list of solutions that meet the needs of the European institutions (covered by TASK-02, TASK-06) and that reflect the best practices from external leaders (covered by TASK-06 and TASK-07). The preferred solutions emerged following a discussion with the EU-FOSSA 2 open source programme office, which then allowed to assess the impact of the implementation of such support for the European institutions.

The study performs a step-by-step approach starting with establishing the needs of EU institutions, then identifying the best practices adopted by the market leaders. These two actions result in recommendations in the form of a way forward for the EU institutions. At the end, it establishes a list of formal requirements that have been sorted by categories and that will serve as a source of predefined requirements to be selected, where applicable, in future Call for Tenders.

Following the analysis of the relevant aspects of the findings from TASK-02 to TASK-08, the deliverables of TASK-05 and TASK-09 define formal requirements for both intellectual property management and support for open source software. Those requirements have been grouped into different categories, in order to insert them in future “Calls for Tenders” that would result in opting for one or more solution providers. They also identify key success factors, metrics, KPIs, as well as minimum criteria to facilitate the creation of a benchmark for future vendor selection via a call for tenders.

The requirements together with the accompanying list of questions to address when launching a Call for Tenders has been elaborated through a sequence of four steps. This sequence of activities is illustrated in the figure below:



In the next sections from Section 2 to 5 the document provides the reader with the main conclusions that have been established during this study from Steps 1 to 4, and that are concluded in this document, officially formalising Step 5 as the Final Report of this Study. Therefore, those sections provide the reader with all useful information about findings and conclusions in relation with the topics associated to each step of the study before to reach the conclusions of this study.

2. STEP 1: IDENTIFICATION OF NEEDS

2.1. IPR NEEDS

2.1.1. INTRODUCTION

This section refers to Task 2 of the EU-FOSSA 2 study also known under "Task 2: List of open source related support requirements for intellectual property support by European institutions, by *institution* and as *a collective*". This part of the study is aimed to gather the observations collected from a targeted audience at European Commission, through a questionnaire submitted via the intranet and by the means of workshops. The inquiries have been conducted based on a structured questionnaire by means of one of the following channels:

- The EU Survey tool, with a limited number of participants (nine people have partaken to the survey)
- Three workshop sessions with the participation of key stakeholders within the European Commission (seven people were interviewed).

This task was aimed at describing the needs identified through the IPR pane of the replies from the survey and concerns the aspects related to intellectual property rights. The selected interviewees to answer this inquiry were using, implementing or partaking to the setting of open source solutions.

For open source intellectual property rights, the key targets of the investigation area involved the identification of:

- the existing initiatives undertaken by the panel of interviewees and survey respondents;
- the level of maturity reached in the field of open source software components configuration;
- the ability to choose among different products or solutions taking into account the intellectual property constraints;
- the problems related to intellectual property faced while implementing new solutions;
- The expectations of the targeted audience towards concrete support and related procedures to be set in place to enhance communication with dedicated legal experts.

The next section provides a summary of the findings relating to that task of the study.

2.1.2. IPR NEEDS, FINDINGS SUMMARY

The current trend observed within the European Commission is a desire to:

- Reach a deeper knowledge of the risks related to the licencing aspects in the use of open source software solutions;
- Inform the partakers of development solutions about the services provided by the Legal support and intellectual property experts within the various DG within the European Commission;
- Develop a corporate policy for the use, integration and development of open source software, taking into account the open source software licensing issues at the very first step of every subsequent project;
- Provide advice on the choice of licences, while supporting the development teams to take initiative and make proposals;
- Set up a fast procedure for licence verifications by legal teams, when the open source software solution opted for is provided by a small-sized company;
- Support the consolidation of the existing open source software catalogue and licences repository (which is in progress with EURECA);
- Allow more flexibility in the use of open source software components that could possibly be integrated in a wider solution;

- Establish a set of guidelines and global policies that support the contribution of technical resources for the user community;
- Make a choice on the automated tools that could be used in order to ease the checks on licence compatibility – (a tool integrating artificial intelligence could be considered)
- Discuss more broadly the potential risks related to reuse of public source code, and consequently take decisions on best practices that should be applied in this field;
- Establish rules and procedures on how to deal with potential bugs or problems that are linked to open source software libraries;
- Foresee how a common approach could be adopted which aims:
    - a) to help finding an adequate solution between the expressed end-user needs and the existing compatibility of the open source software solutions; and consequently, facilitating the adoption of such solutions or tools
    - b) as far as possible, to encourage, within the EU, reusability of the open source software tools that have already been adopted by a specific service;
- Analyse the best ways and approaches in relation with the mutualisation of in-house tools within the European Commission and with other European institutions;
- Build or to share standard procedure and best practices through a unique channel of communication;
- Make internal efforts that aim to raise awareness of stakeholders around the open source software field as a whole;
- Adapt the procurement framework in order to give a chance for small solution providers to contract with the European Commission;
- Provide a structured approach in supporting the choices amongst tools and solutions whilst giving priority to open source software over proprietary software when they share the equivalent functionality and security characteristics;
- Keep on building and spreading a strong common strategy that is dedicated for the European Commission.

2.2. IT SUPPORT NEEDS

2.2.1. Introduction

This section refers to Task 6 of the EU-FOSSA 2 study for the part relating to the "List of open source related support requirements for open source software support by European institutions, by institution and as a collective". This part of the study aims to gather the observations that were collected, through a questionnaire that was submitted through the intranet, from a targeted audience at European Commission, and by means of workshops that were based on the same approach as the one used for Task2.

The enquiries have been conducted based on a structured questionnaire via one of the following channels:

- The EU Survey tool, with a limited number of participants (nine people have partaken to the survey), and
- Three workshop sessions - with the participation of key stakeholders within the European Commission (seven people were interviewed).

This task allowed formulating the needs as identified through the open source software support pane of the survey replies. These were mainly concerned with aspects relating to software management and software support needs.

All interviewees who have been selected for this study, were either using, implementing or partaking in the adoption of open source solutions.

When considering open source software management, the key targets of investigation focused on the identification of:

- the existing initiatives undertaken by the panel of interviewees selected;
- the level of maturity reached in the field of the open source software components configuration;
- the ability to choose among different products or solutions, taking into account the constraints of both software management and support needs;
- the problems relating to software management and support needs while implementing new solutions;
- the best practices to follow in order to allow an easy reuse and sharing of a locally developed solution;
- the expectations of the targeted audience towards concrete support and related procedures to be set in place to enhance communication with dedicated Information Technology (IT) experts.

The next section provides a summary of the findings relating to that task of the study.

2.2.2. IT SUPPORT NEEDS, FINDINGS SUMMARY

- Open source software policy is well-defined at the EU Parliament level, but not yet at the European Commission level.
- One of the key elements that can be pointed out from this study concerns the rules and framing of governance policies around the acquisition of IT products. Concerns have been raised regarding the:
    - constraints relating to the framework contract. This could be a limiting factor for the integration of open source software solutions which have been flagged by a participant as sometimes leading to vendor lock-in;
    - difficulties shouldered by small sized open source service providers, among others, due to the rigid purchasing structure of European institutions which does not encourage, dynamic & streamlined purchasing procedures. This has been mentioned during the enquiries by the participants. Nevertheless, recently a dynamic purchasing procedure has been set up by the procurement team in order to deal with this kind of situation.

      The issue mentioned above could eventually lead to the modification of the "General terms and conditions for information technologies contract" and to the further development of a dynamic purchasing system in order to achieve a level playing field between companies that offer support services and sell software.
- Some of the participants coming from DG JRC – with a legal profile – have expressed the importance that they attach to the broker model. The participants were unaware that such a broker model existed. This model aims to support the internal use of open source software. Evidently, it would have been, and still would be, beneficial to have better communicated the existence of this model to the user-base. The participants also underlined the necessity to review this broker model for the purpose of enhancing the support currently received for open source software.
- A substantive debate could be launched in order to clearly define the specific expectations on open source software support and open source software maintenance. In this respect, it seems necessary to decide which support and maintenance aspects will be handled internally and which will be tackled by an external service provider.
- It has been underlined during the survey, in several ways and by several profiles, that the communication between the technical teams and the legal services could be optimised and facilitated. It is currently not obvious for the concerned parties to know in which context, and by which means, they would require legal support. Furthermore, the technical teams prefer sometimes to even avoid contact with lawyers which could delay the start or the progress of a project.

  This debate should include all aspects related to communication channels between the lawyers and staff members.

- Some participants to the interviews have mentioned that there is a global need to be better informed about a global open source software policy. This policy should include the best practices about management of open source software and tools such as the centralised catalogue, aiming to support concretely the contributions of the technical teams.

  In order to streamline the approach and bring the parties together, it could be useful to set up an open source compliance board that would take the lead on decisions and a common direction regarding the adoption of open source software. The expectations and issues collected and observed vary according to the approach that various teams take in order to procure open source solutions.

  The main items that were highlighted through the study, and that could lead to the establishment of specific procedures, are stated below:

  - Technical teams should be supported in the choice for a solution – either on an open source or a proprietary software – based on objective criteria associated with major benefits, risks and weaknesses.
  - From the onset of an IT project, choices ought to be made between reusing a tool, integrating components of an open source software, including additional developments and developing a solution either in-house or externally.
  - In the event that a team, or department, wish to share a solution within the EC or with other European institutions (including the aspects related to compatibility between licences), it is important that they have at their disposal all the necessary information to support their decision.
  - Technical teams should be aware of:
    - the existing open source software tools developed or integrated in-house,
    - libraries used and eventually updated by other teams within the EC,
    - the internal user communities related to an existing in-house open source software selected or promoted solutions.
  - Technical teams should be assisted in their development activities through a formal contract with the open source software external providers.
  - Determining an efficient way of gathering the problems mentioned by end-users, to take into account their needs and their expectations towards the potential use of open source software.
  - Assessing how to structure the approach for the maintenance of open source software solutions and the potential set-up of a contract in line with such initiatives. The debate around maintenance includes practical aspects such as:
    - Improving corrective maintenance through a better ability to report and track issues, getting patches and corrections as soon as possible, as well as hotfixes and sharing the information with the concerned parties.
    - Improving preventative maintenance through the automation of vulnerability scanning and penetration testing.
    - Improving adaptive maintenance by being able to test, submit and follow-up change requests in a timely manner.
    - Improving maintenance with the implementation of stress/load testing, health monitoring and monitoring of resource consumption.
  - Dealing with communities and determining:
    - what could be the involvement in terms of practical participation to the development and share of common source code;
    - how far the community as a whole can be trusted for the security aspects of a solution;
    - to what extent it is possible to rely on the communities for aspects that are related to:

        - the maintenance of software;
        - the continuous update and enhancement of a solution;
        - the bug fixes.
    - what are the precautions to be taken when interacting with communities and reusing code, libraries and other components?
- Drafting a process to be followed and the criteria that should be taken into account when deciding whether or not to share source code with the rest of the world. This should include the identification of respective responsibilities of the parties implicated in the global process, as well as indications on the level of visibility that the European Commission would aim to reach in this context.
- Considering a specific strategy on how to empower the resources who participate to open source software developments within the European Commission and on how to continuously improve their knowledge in the field of open source software.

3. STEP 2, BEST PRACTICES

3.1. IPR BEST PRACTICES

3.1.1. Introduction

This section relates to the Task 3 of the EU-FOSSA 2 study: "Study the market for leaders and best practices in intellectual property management and deliver a comprehensive report". This part of the study was aimed at gathering a set of observations that were raised from interviews with public organisations, private companies or associations that are very active in the field of open source such as:

- integrators and users;
- in-house solutions developers;
- editors;
- entity sustaining the spread of free and open software;
- or a mix of some profiles mentioned above.

The best practices and experiences collected from these interviews were compared with the issues and expectations that were raised from the participants of this study.

In order to accomplish this task, a research activity has been carried out in order to collect best practices from leaders in the field of open source. This has included collecting documents, research from the internet and participation to webinars.

Furthermore, several interviews have been conducted with both public or private entities that act as leaders in the field of open source software either as:

- innovators, advisers and organisations recognised as a reference in open source software, or as
- intensive users and integrators of solutions aiming to replace the proprietary software use.

The organisations that have been selected are listed below:

- Gendarmerie Nationale Française, in France – [public sector]
- Direction Générale des Finances Publiques, in France (DGFiP) – [public sector]
- Université Catholique de Louvain, in Belgium (UCL) – [public sector]
- INRIA – [public sector]
- Alter Way, in France – [private sector]
- Commission Logiciel Libre Libertis, in France – [private sector]
- Estonian Free and Open-Source Software Association, in Estonia (Alvatal) – [association]
- Flexera[2] – [private sector]
- BearingPoint[3] – [private sector].

[2] Flexera is an American computer software company based in Itasca, Illinois.

[3] BearingPoint is a company based in Amsterdam that delivers management and delivery consulting.

The next section provides a summary of the IPR findings coming out of this Task 3.

3.1.2. BEST PRACTICES, IPR FINDINGS SUMMARY

This section intends to summarise the findings for the final report. Basically, the current study allows the Contractor to summarise the findings as follows:

- Most organisations and individuals are well aware of the licencing aspects of open source software thanks to the publication of handbooks: the guidelines provided by such handbooks should be more closely followed by organisations and result in the implementation of a real governance solution in terms policies, risk assessment, charts, processes, procedures, legal compliance, etc.
- Current status of best practices with IPR reflects a global lack of knowledge from the open source software leaders in the field of IPR.
- Demand for support in the field of intellectual property will increase as the legal problems arise initially.
- There is a strong investment in open source software products from the public sector, especially research institutes that wish to establish a business model.
- There is a real need to manage the licencing aspect of the open source software. This is reinforced by the fact that open source software and proprietary software now coexist in the software market.
- Open source software appears as an easy and non-expensive alternative to proprietary software but there are "hidden" costs related to intellectual property and licence compliancy.
- Some events reveal the importance of the GPL (General Public Licence) that appear as an implicit contract between the two parties (referring to the Artifex V. Hancom decision)[4].
- The Contractor identifies a global need for an IPR/ open source software work methodology integrating properly the role of juridical institutions.
- Globally, the European Commission has a maturity level that is comparable to most of the public and private leaders in this field. However, considering the current state of recent actions as pointed out in this study, it is important to pursue an evolution of maturity through a continuous improvement process.

3.2. IT SUPPORT BEST PRACTICES

3.2.1. Introduction

This section of the study relates to Task 7 of the EU-FOSSA 2 study also known under the name "Task 7:Study the market for leaders and best practices in software and system support". This task aimed to gather a set of observations raised from interviews of public organisations, private companies or associations that are very active in the field of open source, such as:

- integrators and users;
- in-house solutions developers;
- editors;
- organisations promoting free and open software;
- or a mix of some profiles mentioned above.

[4] In reference to the case Artifex vs Hancom, see internet, https://www.linux.com/tutorials/artifex-v-hancom-open-source-now-enforceable-contract/, consulted on November 15th 2019.

The best practices and experiences collected through these interviews have been placed in perspective with several of the issues and expectations that have been raised from the participants of this survey with the European institutions.

Furthermore, several interviews have been conducted with public or private entities that acted as a leader in their field within the open source software domain, namely:

- innovators, advisers and organisation recognised as a reference, or as
- intensive users and integrators of solutions aiming to replace the proprietary software use.

The selection of those entities was made after consultation with the client and in co-operation with the client.

The organisations that have participated in this study are listed below:

- Gendarmerie Nationale Française, in France - [public sector]
- Direction Générale des Finances Publiques, in France (DGFiP) - [public sector]
- Université Catholique de Louvain, in Belgium (UCL) - [public sector]
- Alter Way, in France - [private sector]
- Commission Logiciel Libre Libertis, in France - [private sector]
- Estonian Free and Open-Source Software Association, in Estonia (Alvatal) - [association]

The next section provides a summary of the best practices for IT Support findings.

3.2.2. IT SUPPORT BEST PRACTICES FINDINGS SUMMARY

1. It has been recommended by various external open source software leaders, in order to increase the use of open source solutions inside large organizations, to avoid big-bang transitions from proprietary to open source software and to favor smooth transitions.

   This implies that several transition stages would be necessary, with each aiming to achieve a specific goal. Additionally, in their opinion, the entire transition period should be defined by the highest management level possible.

2. Two aspects should be met together in order to successfully achieve the goal of increasing open source software use within an organization:
   - the focus should be set on building cooperative platforms, interchanging points of views, getting a large adhesion of the whole staff and other collaboration practices around common objectives;
   - it is important to elaborate a common strategy, narrowing down the possible choices, centralizing decisions through decisional bodies and technical boards, supplying common catalogues and decisions tools as well as guidelines.
3. The non-EC open source software leaders interviewed have underlined some of the key success factors that would ease the adoption and maintenance of free and open source solutions. These key success factors could be articulated as follows:
   - investment in human resources more than in equipment;
   - performing continuous updates of the implemented or integrated solutions
   - replacing some of the IT equipment, if necessary, in order to better fit with the needs related to the new solutions adopted;
   - allowing gentle transitions, when necessary, by operating side by side for a while the old and the new solution;
   - raise the awareness of the end users, by supplying ad-hoc trainings when necessary;

- gather the whole organizations' staff around the open source software transition;
- Involve the end users when building open source software solutions and collect their functional needs;
- underline potential gains related to the change, such as the possibility to reduce the budget.

4. What could prevent some technical teams, within European institutions, to use source software solutions more intensely is the fear of technical issues they could face and being unable to deal with.

   This is the same reason why some organizations, like the Gendarmerie Nationale Française, prefer to select mainstream solutions.

5. Concerning interoperability issues and the coexistence between both open source and proprietary products, it has been raised through the interviews with non-EC entities that:
   - although the coexistence of Microsoft products with open source solutions are easily feasible, it is not the case with Oracle and Google products[5].
   - some successful interoperable solutions with Firefox and SAP have been implemented[6], resulting in a multiplatform heavy client associated to a thin client compatible with W3C, able to interoperate with SAP. Such negotiations with big solution providers are made possible thanks to the large size of the institution.
   - proprietary software can be integrated inside virtual machine[7].
6. Regarding the maintenance aspects, as much as possible:
   - the issues and costs related to maintenance aspects of an open source software solution should be treated and assessed in the first stages of the decisional process. This means that aspects such as internal technical teams skills, background and know-how should influence the decisions relating to the formulation of a maintenance services contract with external providers;
   - central decisions should be taken concerning the contractual formulation and aspects of external maintenance services providers.
   - common and streamlined procedures need to be applied, drafted and described for bug fixing.

[5] Issue addressed by the:
- the Gendarmerie Nationale Française
- the DGFiP in France

[6] Information provided by:
- the Gendarmerie Nationale Française
- the Université Catholique de Louvain in Belgium

[7] Observation raised by the association Alvatal in Estonia

4. STEP 3, THE WAY FORWARD

4.1. IPR WAY FORWARD

4.1.1. Introduction

This section relates to the Task 4 of the EU-FOSSA 2 study, also known under the heading: "Task 04: Analyse findings and propose a way forward for intellectual property rights support for open source software that meets the need of the European institutions".

This Task was aimed to gather the results and findings of the previous tasks in combination with a brief examination of the vendor/solution provider landscape to finally issue conclusions and a way forward for the European institutions on the adoption of best practices concerning the management of open source based products within their organisation.

The next section provides an overview of the conclusions and the way forward for the European institutions under the Intellectual Property Right and Licensing perspective.

4.1.2. CONCLUSIONS AND WAYS FORWARD FOR THE EUROPEAN INSTITUTIONS

Based on the previous tasks of this study, sections 1 and 2 of this document contain a summary of the findings and conclusions in terms of the key messages relating to open source.

4.1.2.1. Global open source software IPR Support needs

As a result of the analysis of the needs formulated through the previous task 02, the following new list could be established as a global list considering both IPR and IT Support needs:

1. The need to establish an **Open Source Review Board (OSRB),** as also mentioned as an IT support need in TASK-08, that will act as open source governance at the European Commission in order to establish appropriate IPR open source policies and other governance activities (referring to findings 1, 2, 3, 4, 5, 6, 11, 14, 15, 21, 23, 25, 27, 29, 30).
2. The need for an **appropriate selection and management** of open source licences (referring to findings 1, 2, 3, 7, 8, 9, 12, 13, 16, 22).
3. Need for **internal competence** in relation to IPR and licensing topics (referring to findings 2, 7, 15, 22, 26, 30).
4. Need for **training and raising awareness** in relation with IPR issues related to open source software products (referring to findings 1, 2, 3, 7, 8, 11, 12, 14, 15, 22).

4.1.2.2. List of IPR requirements based on the needs

Req. 1. Implementation of an open source governance through DG JRC

Each European institution should establish an Open Source Review Board (OSRB) that acts as a central decision-making entity including representatives from legal, engineering and product teams, as well as a Compliance Officer.

Good open source governance ensures the effective implementation of the open source policy.

The characteristics[8] of good open source governance are:

- It involves all the departments that are concerned by the use of open source components within the organisation.

[8] Benjamin Jean, *op. cit.*, p. 103.

- It contributes to the improvement of the open source policy.
- It deploys tools and is in charge of technology intelligence.

Such a board ensures cohesion between the different departments and act as a point of reference vis-à-vis these departments. It main responsibilities are as follows:

- It mutualises the open source support.
- It takes rational decisions based on objective criteria.
- It defines the open source policy and the open source licensing policy.
- It promotes the automation of decision-making.

In order for this board to be as efficient as possible, it should be:

- available and responsive;
- supported by the management;
- the only body to be consulted for authorising the use of software bricks under open source licences;
- in a role of information dissemination, extension and training.

Req. 2. Drafting of an open source policy

An important part of the compliance program should consist in the drafting of an open source policy that is brief and written in such a way as to be understandable by the entire staff[9].

This open source policy should contain the essential points for the proper management of open source products and components:

- Developers may only integrate vetted and approved open source components within other software products.
- Before any distribution of software products, an assessment of all software components (proprietary, software received from third party, open source software) should be performed to achieve licensing compliance.
- Approval of open source code consumption should be given on a case-by-case basis: re-use of the same code in another context should be subject to a separate approval procedure.
- Approval should go along with any change to an open source component or snippet in order to take into account any licence evolution related to the release of the new version of the software product through the approval process[10].

The open source licensing policy should complete the open source policy and aims to:

- implement a method for establishing a list of licences that may be used within the European institutions;
- achieve licence compliance with the help of tools, processes and best practices[11];
- mutualise the decisions taken in the context of projects and to promote a good understanding of the issues by employees[12].

[9] Ibrahim Haddad, *op. cit.*, p. 78.

[10] Ibrahim Haddad, *op. cit.*, pp. 77-78.

[11] Benjamin Jean, *op.cit.*, p. 100.

[12] *Ibid.*, p. 97.

Req. 3. Improvement of licence management

The following solutions should be considered in order to improve licence management within the European institutions:

- For pre-approved licences, developers should make decisions on the basis of objective criteria listed in licensing tables.
- For more complex situations, developers should call on the copyright experts from DG JRC so that they can provide their analysis. The developers and copyright experts should then take a reasoned decision by consensus.
- An external service provider, such as a legal office, could provide its expertise, especially in the event of litigation.

Req. 4. Making informed licensing choices

Licences applying to components developed in-house should be chosen on the basis of criteria related to a specific situation. Moreover, they should be adapted to the type of software, the European institution's other software, and the ecosystem in this field, etc. The European institutions should only distribute open source software products that comply with the licences related to the components that make up each software product.

Req. 5. Improving competence in licensing for development and project teams using open source components

This element consists in improving the IPR competence of internal teams through a number of actions that will contribute to enhancing expertise internally.

Req. 6. Implementation of tools for automating licensing decisions

Tools constitute an important aspect of the compliance strategy: the European institutions could adopt tools in order to improve the licensing compliance process[13].

4.1.3. AGREEMENT ON THE PREFERRED SOLUTIONS RESULTING FROM THE DISCUSSION OF THE CONCLUSIONS WITH THE EU-FOSSA 2 OPEN SOURCE PROGRAMME OFFICE

A meeting has taken place on December 19th 2019 at the European Commission DIGIT offices together with the EU-FOSSA 2 open source programme office.

Trasys International (part of the NRB Group) has presented the key messages as collected through findings of previous EU-FOSSA 2 deliverables, i.e. Tasks 02 and 03 for IPR findings and Tasks 06 and 07 for IT Support findings.

4.1.4. IMPACT OF ACCOMMODATING SUCH SUPPORT ON THE EUROPEAN INSTITUTIONS

The development of such solutions within the European institutions will require the following accommodations:

- Within the European Commission, a portal already exists to establish the interface between developers and copyright experts: EURECA. A similar portal should be implemented in other European institutions.
- With the growth of open source, more copyright experts may need to be available in-house to deal with IPR issues.

[13] Ibrahim Haddad, *op. cit.*, p. 116.

REQUIREMENTS	IMPACTS
Req. 1. Implementation of an **open source governance** through DG JRC: Each European institution should establish an Open Source Review Board (OSRB) acting as a central decision-making entity including representatives from legal, engineering and product teams, as well as a Compliance Officer.	**Imp. 1.** Add IPR and licensing aspects in all activities of the OSRB as a central decision-making for IPR and licensing issues, considering three levels of Management Committees (Strategic, Tactical and Operational) and including a continuous improvement spirit in IPR governance activities.
Req. 2. Drafting of an **open source policy**: An important part of the compliance program should consist in the drafting of an open source policy that is brief and written in such a way as to be understandable by the entire staff.	**Imp. 2.** Establish the IPR (licensing) open source policy, ensuring validation by the management of the organisation and communicating the policy to targeted audience (especially staff members and project teams who consume or build open source components).
Req. 3. Improvement of licence management: The following solutions should be considered in order to improve licencing management within the European institutions: ⇨ For pre-approved licences, developers should make decisions on the basis of objective criteria listed in licensing tables. ⇨ For more complex situations, developers should call on the copyright experts from DG JRC so the latter can provide their analysis. The developers and copyright experts should then take a reasoned decision by consensus. ⇨ An external service provider, such as a legal office, could provide its expertise, especially in the event of litigation.	**Imp. 3.** Establish the right balance between internal management of IPR activities and external advising from copyright experts.
Req. 4. Making **informed licensing choices:** Licences applying to components developed in-house should be chosen on the basis of criteria related to a specific situation. Besides, they should be adapted to the type of software, the European institution's other software, the ecosystem in this field, etc. The European institutions should only distribute open source software products that comply with the licences related to the components that make up each software product.	**Imp. 4.** Facilitate communication between open source software /IPR parties. To initiate the setting of a dedicated platform that will ease the communication between all open source software /IPR actors.
Req. 5. Improving **competence** in licensing for development and project teams using open source components: It consists in improving the IPR competence of internal teams through a number of actions that will contribute to enhance expertise internally.	**Imp. 5.** Build and improve internal expertise. To ensure the presence of internal competence centres with open source software/IPR experts to manage the projects. **Imp. 6.** Organisation of training sessions on a regular basis: DG JRC should continue to organise

	training sessions for staff on a regular basis. The European institutions can also call on an external service provider to do so.
Req. 6. Implementation of tools for **automating licensing decisions:** Tools constitute an important aspect of the compliance strategy: the European institutions could adopt tools in order to improve the licensing compliance process.	**Imp. 7.** Choosing one or multiple tools according to some specific criteria. **Imp. 8.** Ensuring the adequate deployment of the tools, including maintenance and updates.

4.2. IT SUPPORT WAY FORWARD

4.2.1. INTRODUCTION

This section relates to the Task 8 of the EU-FOSSA 2 study, also known under "Task 08: Analyse findings and propose a way forward for open source software support requirements that meets the needs of the European institutions".

This Task aimed to gather the results and findings of the previous tasks in combination with a brief examination of the vendor/solution provider landscape to finally issue conclusions and a way forward for the European institutions.

The next section provides an overview of the conclusions and the way forward for the European institutions concerning IT support requirements for open source solutions.

4.2.2. CONCLUSIONS AND WAY FORWARD FOR THE EUROPEAN INSTITUTIONS

Based on the previous tasks of this study, sections 1 and 2 of this document contain a summary of the findings and conclusions in terms of key messages relating to open source.

4.2.2.1. Global open source software IT Support needs

As a result of the analysis of the needs of the EU institutions as formulated in the task 06, the following new list could be established as a global list considering the IT Support needs.

1. The EU institutions expressed the need of having an **Open Source Review Board (OSRB)** that will act as open source governance at European Commission in order to establish appropriate open source policies, define and implement an appropriate open source framework including leadership activities in the field of open source, risk management assessments, awareness and training material, audit program, central decision relating to contracting development and/or maintenance services with external providers, supporting the development of cooperative platforms to facilitate the communication between the developers community and their stakeholders, and continuous improvement of open source processes and procedures (referring to findings 1, 2, 3, 4, 5, 6, 11, 14, 15, 21, 23, 25, 27, 29, 30).
2. Another need of the EU institutions is for customers **to access** the correct **open source software /IPR skills** at the consulted providers and to have access to the whole picture of skills through open source software /IPR Broker organisations with a good enough Service Level Agreement in order to get the desired level of service (referring to findings 5, 21, 24, 25).
3. There is a need **to** ensure the presence of an **internal competence centre** of open source software /IPR experts to manage the projects and to continuously improve the open source software expertise within the team through integration of appropriate open source software experts and through knowledge handover from external providers to the team for each project (referring to findings 15, 21, 24, 26, 29).

4. There is a need **to** ensure globally an **open source software /IPR Quality Insurance** for European institutions and final customers (referring to findings 20, 30).
5. There is a need to manage properly the **open source software development and delivery** that are delivered by solutions providers through appropriate procurement processes and procedures (referring to findings 24, 27).
6. Furthermore there is a need to **automate activities** like open source software quality checks, legal/licencing compliance, … (referring to findings 2, 9, 16).

4.2.2.2. List of requirements based on the needs

Based on the list of needs, the Contractor recommends addressing the following specific requirements when initiating any action like a Call for Tenders in relation to open source software services:

Req. 1. **Open source software governance implementation:** To ensure alignment of the service provider with the components of the open source software governance of the European institutions: this should include the consideration of the global open source software policy, communities interaction policy, risk assessment, leadership and support, internal audit program, incident management, training and continual improvement. Such governance should follow a Plan-Do-Check-Act (PDCA) mechanism.

Req. 2. **Provide access to the right expertise to solve bugs and problems**: To provide the European Commission with easier access to small open source software /IPR Broker organisations for support and maintenance activities. Such access to the open source software services of small organisations will be made possible thanks to the use of a contractual agreement with a "Broker" organisation that will be linked with smaller organisations that can provide the required open source software expertise.

Req. 3. **Provide guarantee of service** through better access to small organisations: To establish a list of specific open source software requirements (level of expertise, kind of services and intervention in the project, specific key performance indicators and success factors):

- Service Level Agreement between European Commission and the Service Provider;
- Call for Brokers increasing the effectiveness and efficiency of the small actors through an intermediary organisation;
- Permanent monitoring of services under delivery process;
- Evaluation of delivered open source software services;
- Identification of a complain process for use by European Commission;

Req. 4. Elaboration of a specific **desired maturity level** of the developed code and associated actions including code documentation, code review, pen-testing, code auditing, code crossed review, …

Req. 5. To improve open source software **Competence of internal teams** through a number of actions that will contribute to enhance the expertise inside the European institutions.

Outside of those requirements, one could also address a number of questions before starting an open source software project in order to help understand whether or not the switch to Open Source Solutions is advantageous.

4.2.3. AGREEMENT ON THE PREFERRED SOLUTIONS RESULTING FROM THE DISCUSSION OF THE CONCLUSIONS WITH THE EU-FOSSA2 OPEN SOURCE PROGRAMME OFFICE

A meeting has taken place on December 19th 2019 at European Commission DIGIT together with EU-FOSSA 2 open source programme office.

Trasys International (part of the NRB Group) has presented the key messages as collected through the findings from the previous EU-FOSSA 2 deliverables, i.e. Tasks 02 and 03 for IPR findings and Tasks 06 and 07 for IT Support findings.

During the meeting of 19th December 2019, the EU DIGIT EU-FOSSA 2 open source programme office has globally pointed out one dominant requirement among all key messages, which is about the need for "**Ensuring access to the right expertise to solve bugs and problems when they occur**".

All the other conclusions and recommendations of the way forward from section 4 were accepted by the EU DIGIT EU-FOSSA 2 open source programme office and will need to be further analysed by the European Commission for their implementation through a phased approach that will be privileging a step-by-step "smooth transition" approach and will be avoiding a big-bang migration from proprietary to open source software.

4.2.4. IMPACT OF ACCOMMODATING SUCH SUPPORT ON THE EUROPEAN INSTITUTIONS

Considering the best practices coming from open source leading organisations and considering how those best practices could answer the needs of the European institutions, this study allowed elaborating a number of requirements that are listed in section 4 and that will generate some level of impact to the existing structure in place if the European Commission decides to manage those requirements by adopting an action plan and by ensuring its implementation.

The implementation of the action plan will generate an impact on the European Commission's structure. The European Commission will need to adapt its international organisation with tools and means that will facilitate a smooth transition to open source. The European Commission shall also consider the following list of requirements to be submitted to its open source software service providers in order to ensure their best contribution to the open source software governance of the European Commission. The next table provides a list of such requirements with a description of the possible impacts for the European institutions:

REQUIREMENTS	IMPACTS
Req. 1. Open source software Governance Implementation: To align with and support the established components of the open source Software governance including a global policy, communities interaction policy, risk assessment, leadership and support, internal audit program, incident management, training and continual improvement around Plan-Do-Check-Act (PDCA) framework.	**Imp. 1.** Setup an Open Source Review Board operating as central decision making for open source software /IPR. For all EU institutions, to establish an « Open Source Review Board » acting as a central decision-making entity including representatives from legal, engineering and product teams, as well as a Compliance Officer. **Imp. 2.** Setup Management Committees (Strategic, Tactical, Operational). To organise a regular communication between copyright specialists and open source software developers teams at all levels (strategic, tactical and operational).  **Imp. 3.** Develop a Continuous Improvement spirit in all open source software /IPR activities. Make sure that any activity will be subject to improvement year after year through adapted Managerial review of the processes and thanks to an internal audit plan and program.
Req. 2. Provide access to the right expertise to solve bugs and problems: To fill the gap due to the lack of skills of individual providers. To	**Imp. 4.** Extend relations with sources of expertise in two ways:

REQUIREMENTS	IMPACTS
provide European Commission with a contractual agreement through Broker contracting with Support & Maintenance open source software /IPR Broker organisations.	⇨ Extending relationship through more interactions of internal developers with open source software communities. ⇨ Contracting with brokers which are themselves contracting with open source software SMEs to get the right expertise and bugs solving solution.
Req. 3. **Provide guarantee of service:** To establish a list of specific open source software requirements (level of expertise, kind of services and intervention in the project, specific key performance indicators and success factors): ⇨ Service Level Agreement between European Commission and the Service Provider; ⇨ Call for Brokers increasing the effectiveness and efficiency of the small actors through an intermediary organisation; ⇨ Permanent monitoring of services under delivery process; ⇨ Evaluation of delivered open source software services; ⇨ Identification of a complain process for use by European Commission;	**Imp. 5.** Define Key Performance Indicators and levels of performance with external contracted service providers. The identification of appropriate KPIs should be addressed in a further stage by the EU-FOSSA 2 open source programme office in order to be submitted to external providers.
Req. 4. Elaboration of a **specific desired maturity level** of the developed code and associated actions including code documentation, code review, pen-testing, code auditing, code crossed review, …	**Imp. 6.** Identify quality target, globally and project specific. To establish, document and publish the desired level of quality in produced open source software codes and ensure an open source software /IPR Quality Insurance for European institutions and final customers.
Req. 5. To improve open source software **Competence of internal teams** through a number of actions that will contribute to enhance expertise internally.	**Imp. 7.** Build and improve internal expertise. To ensure presence of internal competence center with open source software /IPR experts to manage the projects. **Imp. 8.** Maintain permanent training activity. To setup internal training sessions regularly to allow increasing the knowledge, know-how and competences of internal IPR/ open source software experts. **Imp. 9.** Facilitate communication between open source software /IPR actors. To initiate the setting of a dedicated platform that will ease the communication between all open source software /IPR actors.

5. STEP 4, CATEGORIES AND FORMAL REQUIREMENTS

5.1. IPR CATEGORIES AND FORMAL REQUIREMENTS

5.1.1. ANALYSE RELEVANT ASPECTS OF THE FINDINGS FROM EARLIER TASKS

Previous tasks have led to the definition of a series of requirements for intellectual property support that are required by European institutions:

1. TASK-02 contributed to the identification of the needs of the various European institutions (the European Commission, the European Parliament and the Council of the European Union) via interviews within these institutions.
2. TASK-03 aimed to gather best practices and lessons learned in intellectual property management from external leaders active in the field of open source within both the public and private sectors.
3. TASK-04 led to the creation of a list of solutions that were based on the needs of the European institutions and implemented following best practices of external leaders.

TASK-04, the content of which is derived from TASK-02 and TASK-03, contains a summary of the findings and conclusions related to intellectual property rights support for open source software. Below are the findings of this task for the record.

5.1.1.1. Global open source software IPR and IT Support needs

As a result of the analysis of the needs that were formulated in TASK-02, the following global list could be established considering both IPR and IT Support requirements:

5. A need to establish an **Open Source Review Board (OSRB**). This is also mentioned as an IT support need in TASK-08, that will act as an open source governance framework for the European Commission in order to establish appropriate IPR open source policies and other governance activities (referring to findings 1, 2, 3, 4, 5, 6, 11, 14, 15, 21, 23, 25, 27, 29, 30).
6. A need for an appropriate **selection and management of open source licences** (referring to findings 1, 2, 3, 7, 8, 9, 12, 13, 16, 22).
7. A need for **internal competence** in relation to IPR and licensing topics (referring to findings 2, 7, 15, 22, 26, 30).
8. A need for **training and raising awareness** in relation with IPR issues related to open source software products (referring to findings 1, 2, 3, 7, 8, 11, 12, 14, 15, 22).

5.1.1.2. IPR requirements List Based on the Needs

Req. 1. The Creation of an open source policy

An important part of the compliance program should consist in the creation of an open source policy that is brief and written in such a way as to be understandable by the entire staff[14]. An open source licensing policy should complete the open source policy[15].

Req. 2. The Implementation of an open source governance through DG JRC

[14] Ibrahim Haddad, with contributions from Shane Coughlan and Kate Stewart, Open source compliance in the enterprise, Sponsored FOSSID for the Open Compliance Summit 2018, The Linux Foundation, 2nd Edition 2018, p. 78.

[15] *Ibid.*, p. 97.

Each European institution should establish an Open Source Review Board (OSRB) that acts as a central decision-making entity that should include representatives from legal, engineering and product teams, as well as a Compliance Officer.

Req. 3. The Improvement of licence management

According to the Contractor, the following solutions should be considered in order to improve licence management in the European institutions:

- For pre-approved licences, developers should make decisions on the basis of objective criteria that should be listed in the licensing tables.

- For more complex situations, developers should call on the copyright experts from **DG JRC** so that they can provide their analysis. The developers and copyright experts should then take a reasoned decision by consensus.

- An external service provider, such as a legal office, could provide its expertise, especially in the event of litigation.

Req. 4. Making informed licensing choices

Licences applying to components developed in-house should be chosen on the basis of criteria that are related to a specific situation. Furthermore, the licenses should be adapted to the type of software, the European institution's current software, and the IT ecosystem in this field, as an example. The European institutions should only distribute open source software products that comply with the licenses related to the components that make up each software product.

Req. 5. Improving competence in licensing for development and project teams using open source components

This consists in improving the IPR competency of internal teams through a number of actions that will contribute to improving internal expertise.

Req. 6. Implementation of tools for automating licensing decisions

Tools constitute an important aspect of the compliance strategy: the European institutions could adopt tools in order to improve the licensing compliance process[16].

5.1.2. ANALYSE AND GROUP THE REQUIREMENTS OF THE EUROPEAN INSTITUTIONS FOR IPR SUPPORT INTO CATEGORIES

5.1.2.1. Initially identified categories

Through previous tasks, the two following categories were investigated in which all findings could be categorised:

[16] Ibrahim Haddad, *op. cit.*, p. 116.

5.1.2.1.1. Policy, Coordination and Communication

- Creation of open source policies;
- Implementation of an open source governance through DG JRC;
- Improvement of licence management.

5.1.2.1.2. Supporting and Maintenance

- Making informed licensing choices;
- Improving competence in licensing for development and project teams using open source components;
- Implementation of tools for automating licensing decisions.

5.1.2.2. Extended list of categories / subcategories

When analysing further the previous findings and also considering the best practices as defined by leaders on the market and reputed organisations (including ISO standards, OWASP references and external leaders publications on the market), findings could be extended through the following additional categories which might be more specific than the two above:

5.1.2.2.1. Governance

Most management systems are described with guidelines coming from ISO standard for best practices in their implementation. Those best practices refer to the implementation of a number of Governance components including:

- Defining a compliance strategy and program[17];
- Assigning roles and responsibilities for users involved in compliance contribution[18];
- Drafting IPR Policies for open source software: open source software Policy, open source software Licensing Policy, open source software Distribution Policy;
- Implementing open source compliance processes[19];
- Setting up a source code publishing process[20]:
  - Choosing a publication model;
  - Preparing source code packages;
  - Using a pre-publication checklist;
  - Publishing the source code;

[17] Ibrahim Haddad, *op. cit.*, p.30.

[18] *Ibid.*, p. 46.

[19] Ibrahim Haddad, *Publishing Source Code for FOSS Compliance: Lightweight Process and Checklists*, Linux Foundation, 2012, p. 1.

[20] *Ibid.*, p. 2-5.

- Using a post-publication checklist.

- Creating the Open Source Review Board (OSRB)[21]:
  - Approving the consumption of open source components;
  - Providing advice about open source licensing through licence playbooks, licence compatibility matrix, licence classification, software interaction methods, checklists[22].
  - Reviewing and approving updates to end-user documentation;
  - Contributing to the creation and the management of the compliance program.
- IPR Risk Assessment (licensing risk register, licensing risk identification, measurement, evaluation, treatment, residual risks, …);
- IPR Supporting for open source software;
- IPR analysis, evaluation and licensing process (including dealing with licensing issues, relicensing, licence compatibility, IPR asset management);
- Implementation, management and continual improvement of the licensing process;
- Managing compliance inquiries[23].

5.1.2.2.2. External IPR Supporting Management according to ISO37500:2014

Outsourcing management if further described by the ISO 37500:2014 standard providing guidance on the following topics:

- Good outsourcing Governance for the mutual benefit of client and provider;
- Flexibility of outsourcing arrangements, accommodating changing business requirements;
- Identifying risks involved with outsourcing;
- Enabling mutually beneficial collaborative relationships.

5.1.2.2.3. Internal IPR Supporting Management

Coming from the findings established in previous tasks of this study, training and internal open source software competence development could be further developed through activities including:

- Training;
- Collaborative platform to facilitate communication between stakeholders[24], ensuring communication for both internal and external compliance.
- Training and awareness-raising about recognised or possible licensing compliance issues for existing teams;
- Handover to internal teams.

[21] Ibrahim Haddad, with contributions from Shane Coughlan and Kate Stewart, *Open source compliance in the enterprise*, Sponsored FOSSID for the Open Compliance Summit 2018, pp. 53-54.

[22] Ibrahim Haddad, *Practical Advice to Scale Open Source Legal Support*, Linux Foundation, 2013, p. 4.

[23] Ibrahim Haddad, with contributions from Shane Coughlan and Kate Stewart, *Open source compliance in the enterprise*, Sponsored FOSSID for the Open Compliance Summit 2018, The Linux Foundation, 2nd Edition 2018., p. 120.

[24] Ibrahim Haddad, *op. cit.*, p. 40.

5.1.2.2.4. Information and knowledge

Information and knowledge management is a necessary foundation to any team-related activity. It has also been mentioned in previous tasks as an essential need for any organisation having to manage internal or external activities relating to open source software development and production. Such activities include:

- Setting up a collaborative platform to allow communication between developers and stakeholders including:
  - Weblog;
  - Chat service;
  - Link with legal experts;
  - Project repository from design to operations;
- Definition of a level of expertise, IPR-related functions for open source software, IPR job description for open source software.

5.1.2.2.5. Automated tools

Automated tools have been defined as findings in the previous tasks and they refer to best practices in intellectual property management of open source software.

- Adopting automated tools to ease the checks on licencing compatibility including for example source code identification tool, project management tool, software bill of material (BOM) difference tool, linkage analysis tool;
- Automating activities as much as possible for all aspects relating to IPR management.

5.1.3. DOCUMENT REQUIREMENTS IN THE MANNER FOR FINAL INPUT TOWARDS A CALL FOR TENDERS

5.1.3.1. Table of Requirements for Tenders

Considering the fact that European institutions will involve external providers to deliver services that will fulfil their requirements, it is important to ensure that such requirements are expressed in a S.M.A.R.T. way meaning that those requirements are:

1. Specific: written out clearly with concise goals
2. Measurable providing the ability to track the progress
3. Achievable set in a challenging mode, however with achievable goals
4. Relevant establishing goals that are relevant to the open source software project life plan
5. Time-based making sure that goal has a target finish time attached

The following table lists the requirements to be submitted to external providers with questions to clarify the positioning of the service provider in relation to the requirement. Those requirements are reformulated to be more concretely understood by service providers and are ranged by categories. In practice, at the time to launch the call for tenders, it will be necessary to add columns to be filled in by service providers in order to indicate their level of compliance with the requirement (Fully, Partially compliant, or No compliance).

CATEGORY	REQUIREMENTS	Questions to be addressed
Governance	➢ IPR and Licensing compliance program; ➢ Roles and responsibilities; ➢ Policies for licence compliance: ▪ Open source software IPR/Licensing Policy; ▪ Open source software Distribution Policy; ➢ Implementing open source compliance processes; ➢ Setting up a source code publishing process: ▪ Choosing a publication model; ▪ Preparing the source code packages; ▪ Using a pre-publication checklist; ▪ Publishing the source code; ▪ Using a post-publication checklist; ➢ Open Source Review Board (OSRB) including IPR / Licensing; ➢ IPR Risk Assessment (licensing risk register, licensing risk identification, measurement, evaluation, treatment, residual risks, …);	1. What is your expertise in creating an open source software compliance program? a. Do you advise on implementing open source governance for achieving licence compliance? b. Do you advise on implementing open source compliance processes? c. Do you advise on setting up a source code publishing process? d. Can you advise on implementing a governance framework that will include the following components: open source software policy, open source software licensing policy, distribution policy, OSRB, IPR risk assessment, IPR supporting, IPR licensing process? 2. In case you cannot provide advice on all of the above-mentioned elements, what alternative solutions do you propose in order for the European institutions to improve their Governance? 3. Can you provide information about your vision of open source governance, and especially how it should help the European institutions manage their intellectual property and achieve compliance? 4. How do you ensure the transfer of knowledge to European institutions so that they can implement the governance internally? 5. How do you propose to manage compliance inquiries?

CATEGORY	REQUIREMENTS	Questions to be addressed
	➢ IPR Supporting for open source software; ➢ IPR analysis, evaluation and licensing process; ➢ Licensing process continual improvement.	
External IPR Supporting Management	➢ Good outsourcing Governance for the mutual benefit of client and provider; ➢ Flexibility of outsourcing arrangements, accommodating changing business requirements; ➢ Identifying risks involved with outsourcing; ➢ Enabling mutually beneficial collaborative relationships.	6. How do you handle and assign the ownership of: a. the supplied software (including all associated intellectual property rights with no restrictions on the purpose and type of use)? b. the source code (which may be studied by the public organisation or a third party for testing, training or other purposes)? c. the software which may be modified (by the public organisation or a third party in order to tailor it to its own needs)? d. and the software that can be distributed (with or without modifications by the public organisation to any party of its choice under the same terms and conditions)? 7. What is your approach regarding the management of IT Supporting activities? 8. Which clauses do you provide to ensure flexibility in the outsourcing arrangements? 9. How do you describe the IT supporting services in terms of time of intervention, volume of effort that you will deploy, level of service management? 10. How will you evaluate the customer satisfaction and pursue activities to ensure a complete customer satisfaction?
Internal IPR Supporting Management	➢ Training; ➢ Collaborative platform to facilitate communication between stakeholders; ➢ Training and awareness-raising for existing teams; ➢ Handover to internal teams.	11. How will you ensure having the appropriate experts to provide the required level of expertise and how will those experts interact with the internal developers? 12. Which activities do you foresee from your catalogue to improve the competence in intellectual property of internal developers at European Commission Software Development Team? 13. How will you organise the transfer of knowledge from your organisation to the Software Development Team? 14. What kind of training programs in the field of intellectual property management for open source software do you offer?

CATEGORY	REQUIREMENTS	Questions to be addressed
		15. How will you ensure the continued level of service in the event of people turn-over within your team?
Information and knowledge management	➢ Setting up a collaborative platform to allow communication between developers and stakeholders including: ▪ Weblog; ▪ Chat service; ▪ Link with legal experts; ▪ Project repository from design to operations; ➢ Definition of level of expertise, IPR-related functions for open source software, IPR job description for open source software.	16. What kind of collaborative platform do you provide that allows communication between developers and stakeholders? 17. Is this platform going to be implemented at the EC site for use by the Software Development Team and free of charge to the EC or is there an associated cost? In case there is a cost, how is it included in your proposal? 18. How do you plan to implement that platform in the context of the open source software project / services to be delivered and under which conditions? Under which conditions will the platform stay in place for use by the customer after the end of the project/contract? 19. How will this platform serve as a communication solution between open source software developers and IPR/Licensing legal experts? 20. How do you ensure the security of that collaborative platform? Will it be located in Europe?
Automated tools management	➢ Adopting automated tools to ease the checks on licencing compatibility; ➢ Automating activities as much as possible for all aspects relating to IPR management.	21. Which automated tools can you provide from your current catalogue of automated tools? 22. Which ones will you produce or develop that will be made available in the context of this mission among the following list of tools: source code identification tool, project management tool, software bill of material (BOM) difference tool, linkage analysis tool? 23. How do you plan to implement these tools within the environment of the Software Development Team? 24. Will the tools stay in place for use by the customer after the end of the project/contract? 25. How secure will those tools be?

5.1.3.2. Additional considerations[25]

In first instance, the Contractor recommends NOT to enforce definitive requirements in Call for Tenders, but rather to determine whether the service provider is currently compliant or not and, if not, whether it will become compliant

[25] In practice, when considering a specific "OSS services Call for Tenders", it will be convenient to address the formal requirements under the form of a worksheet table in which an additional column will indicate the relevance for the customer of each question (applicable or not) and other columns will be at the disposal of the service providers to express their level of compliance with regards to the requirement and will add descriptive explanation to illustrate his answer.

by the end of the project or after a specific period of time to be defined according to the context (project for development of an open source software application, maintenance service activity, bug fixing support, …).

For each requirement, it will be important to ask the service providers to confirm their position as being:

1. **Fully compliant** (the customer will add an "X" in this column if he confirms full compliance with the specified requirement; they will also justify their choice by adding comments in the last column).
2. **Partially compliant** (the customer will indicate his percentage of compliance in this column in case of partial compliance; he will also justify their choice by adding comments in the last column as well as explain how he will adapt himself to cover the gap).
3. **Not compliant** (the customer will add an "X" in this column if they are not compliant at all for this requirement; they will justify their position by adding comments in the last column as well as explaining how they suggest covering this requirement).
4. **Comments:** the customer will add comments in this column to clarify their position:
    - Either by providing evidence of full compliance;
    - Either by providing evidence of partial compliance and explaining optional suggestions for covering the non-compliant activities by compensation measures to reach a better level of compliance;
    - Either by justifying the non-compliance status with arguments for non-applicability or compensating measures.
5. **In all cases,** the service provider should be authorised to propose adding, modifying and/or cancelling a requirement by justifying themselves on that position. The European Commission will then analyse the comments of all service providers in order to perform a lessons learned and investigate possible adaptations of the list of requirements:
    - Either by removing a requirement in the event that a particular requirement has been systematically declined by all service providers; meaning that such a requirement is probably not acceptable nor achievable and should then be considered for reformulation or just removed from the list.
    - Either by modifying the formulation of a requirement for which several service providers would suggest modifications and/or would indicate partial or no compliance.
    - Either by adding new requirements in case that any missing requirements would be mentioned by one or several service providers.

Ideally, the Call for Tenders will also provide the possibility for candidate Tenders to make suggestions and provide comments globally or specifically per requirement in the context of the Call for Tenders.

5.1.4. DEFINING KEY SUCCESS FACTORS, METRICS AND THE MINIMUM CRITERIA TO HELP SET A BENCHMARK FOR FUTURE VENDOR SELECTION VIA A CALL FOR TENDERS

The next table revisits the IPR / Licensing requirements with the indication of possible Success Factors and Key Performance Indicators/Minimum Criteria in 3rd and 4th columns. It's to be noted that such information is indicative, to be used as a basis before tailoring the European Institution's requirements list more accurately once the Go Ahead will be given to launch a Call for Tenders.

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
Governance	➢ IPR and Licensing compliance program; ➢ Roles and responsibilities;	Provider has expertise, methodology and accompanying tools to implement all	Developed open source software Policy. Risk Assessment methodology implemented

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
	➢ Policies for licence compliance: ▪ Open source software IPR/Licensing Policy; ▪ Open source software Distribution Policy; ➢ Implementing open source compliance processes; ➢ Setting up a source code publishing process: ▪ Choosing a publication model; ▪ Preparing the source code packages; ▪ Using a pre-publication checklist; ▪ Publishing the source code; ▪ Using a post-publication checklist; ➢ Open Source Review Board (OSRB) including IPR / Licensing ; ➢ IPR Risk Assessment (licensing risk register, licensing risk identification, measurement, evaluation, treatment, residual risks, …); ➢ IPR Supporting for open source software; ➢ IPR analysis, evaluation and licensing process; ➢ Licensing process continual improvement.	components of the open source software Governance.	and applied to all applicable domains. Committed Budget and resources. OSRB components reviewed by the management. Implemented licensing process for improvement.
External IPR Supporting Management	➢ Good outsourcing Governance for the mutual benefit of client and provider; ➢ Flexibility of outsourcing arrangements, accommodating changing business requirements; ➢ Identifying risks involved with outsourcing;	Identification of open source software services specifications for outsourcing. Identification of level of service required and performance. Monitoring of delivered services	Coherence between the list of proposed and delivered services. The performance of delivered services in line with the contractually agreed tolerance zones. Existence of specific clauses in outsourcing contract for contract adaptation.

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
	➢ Enabling mutually beneficial collaborative relationships.	Renegotiation of outsourcing in function of deviation between performance specifications and delivery.	
Internal IPR Supporting Management	➢ Training; ➢ Collaborative platform to facilitate communication between stakeholders; ➢ Training and awareness-raising for existing teams; ➢ Handover to internal teams.	Existing and operational training catalogue. Implemented open source software collaborative platform. Built list of open source software expertise areas and internal needs. Developed process for knowledge handover to internal staff.	Review on a yearly basis of the training needs based on open source software market evolution. Involvement of more than 80% of staff in the collaborative platform since last month. A good balance between the number of open source software experts and the project needs (in the critical path). Implemented process for knowledge handover to internal staff.
Information and knowledge management	➢ Setting up a collaborative platform to allow communication between developers and stakeholders including: ▪ Weblog; ▪ Chat service; ▪ Link with legal experts; Project repository from design to operations; ➢ Definition of level of expertise, IPR-related functions for open source software, IPR job description for open source software.	Implemented collaborative platform with communication and coordination features for information knowledge management and coordination activities between open source software staff.	Operational collaborative platform and involvement of more than 80% staff during last 3 months.
Automated tools management	➢ Adopting automated tools to ease the checks on licencing compatibility; ➢ Automating activities as much as possible for all aspects relating to IPR management.	Established list of needs for automated tools. Identified tools corresponding the needs.	Implemented tools and delivery of outputs on an adhoc basis.

5.2. IT SUPPORT CATEGORIES AND FORMAL REQUIREMENTS

5.2.1. ANALYSE RELEVANT ASPECTS OF THE FINDINGS FROM EARLIER TASKS

All previous tasks have contributed to the following approach in order to determine requirements of the European institutions regarding system support:

1. The first step started with the task 06 and contributed to the identification of the needs of European institutions through interviews within the various EU establishments (Commission, Parliament, Council).
2. The second step was accomplished through task 07 which involved the Identification of best practices of market leaders who are active in the field of open source software.
3. In a third step, task 08 provides recommendations, through the adoption of best practices (as those identified in Task 7), coming from market leaders in order to respond to the European Institution's needs (as those that have been identified in Task 6).

Task 08, based on the outputs of tasks 06 and 07, contains a summary of the findings and conclusions in terms of key messages relating to open source. These findings are presented for record in the next subsections.

5.2.1.1. Global open source software IT Support needs

Following the analysis of the EU Institutions needs, as formulated in task 06, the following sections could be considered as a summary for all IT Support needs:

1. Referring to findings 1, 2, 3, 4, 5, 6, 11, 14, 15, 21, 23, 25, 27, 29, and 30, there is a clear need to have an **Open Source Review Board (OSRB)** that will act as an open source governance for the European Commission. This is required in order to establish:
    - the appropriate o**pen source policies**, and
    - the definition and implementation of an appropriate open source centralised decision taking authority.

This Authority, in turn, is concerned with issues such as:

- leadership activities, in the field of open source,
- risk management assessments,
- awareness and training material,
- audit program,
- central decisions relating to out-sourcing and/or maintenance services with external providers,
- supporting the development of cooperative platforms to facilitate the communication between the developer's community and their stakeholders, and
- continuous improvement of open source processes and procedures

2. There is a need for customers to **access the right open source software /IPR skills** with the designated providers and to have access to the whole range of skills through open source software /IPR Broker organisations with appropriate Service Level Agreement in order to get the desired level of service (referring to findings 5, 21, 24, 25).
3. There is a need to ensure the presence of an **internal competence** centre of open source software /IPR experts to manage the projects and to continuously improve the open source software expertise within the team. This should be supported by integration of appropriate open source software experts and transfer of knowledge from external providers to the team for each project (referring to findings 15, 21, 24, 26, 29).

4. There is a need to ensure overarching open source software /IPR **Quality Assurance** for European institutions and final customers (referring to findings 20, 30).
5. There is a need to **manage the open source software development and delivery** by solutions providers through appropriate procurement processes and procedures (referring to findings 24, 27).
6. There is a need to **automate activities** like open source software quality checks, legal/licencing compliance, … (referring to findings 2, 9, 16).

5.2.1.2. List of requirements based on the needs

When consulting the publication of SMILE organisation called "Understanding open source and free software", the following statement appears concerning Support Requirement[26]: *"What do we mean by support? The capacity to provide help in using the programme and correcting the programme, where necessary."*

Based on the list of needs, the Contractor recommends addressing the following specific requirements when initiating any action such as a Call for Tenders in relation with open source software services:

Req. 6. **Open source software Governance** Implementation: To align with and support the established components of the open source software Governance Board defining an overarching policy, community interaction policy, risk assessment, leadership and support, internal audit program, incident management, training and continuous improvement through a Plan-Do-Check-Act (PDCA) framework.

Req. 7. Provide **access to the right expertise** to solve bugs and technical issues: To bridge the gap linked to the limitations of individual service providers.

Req. 8. Provide **guarantee of service:** To provide the European Commission with a contractual agreement through Broker contracting with Support & Maintenance open source software /IPR Broker organisations. This shall be accompanied with specific measures including:

- Service Level Agreement between European Commission and the Service Provider;
- Call for Brokers to improve the communication between subcontractors and a substantially larger organisation;
- An appropriate and permanent monitoring process of services delivered by the service providers;
- Evaluation of delivered open source software services;
- Identification of a complaint process to be used by the end-user;

Req. 9. Identification of a specific **target maturity level** of the developed code and associated actions including, for instance, code documentation, code review, penetration testing, code auditing, code crossed review, …

Req. 10. To improve open source software **Competence of internal teams** through a number of actions that will contribute to enhancing expertise internally.

[26] SMILE, "Understanding open source and free sotware", see internet: https://www.smile.eu/en/publications/list-white-papers, consulted on 20/01/2020, p. 29.

5.2.2. ANALYSE AND GROUP THE REQUIREMENTS OF THE EUROPEAN INSTITUTIONS FOR SYSTEM SUPPORT INTO CATEGORIES

5.2.2.1. INITIALLY IDENTIFIED CATEGORIES

The following two categories are the result of the previous tasks and deliverables. Task 4 and Task 8 both concluded that most findings could be assigned to one of the two following categories:

5.2.2.1.1. Policy, Coordination and Communication

- Open source software Policy regarding interaction of developers with open source software Communities;
- Corporate Policy for using, integrating, developing open source software and managing licencing issues.

5.2.2.1.2. Supporting and Maintenance

- Getting access to the right expertise to solve bugs and problems;
- Call for Brokers so as to improve the communication between subcontractors and the end-user;
- Establishment of a Service Level Agreement between EC and the Service Provider.

5.2.2.2. EXTENDED LIST OF CATEGORIES / SUBCATEGORIES

When analysing further the previous findings and also considering the best practices as defined by leaders on the market and reputed organisations (including ISO standards, OWASP references and external leaders publications on the market), the findings could be extended through the following additional categories which might be more specific than the two above:

5.2.2.2.1. Governance

Most management systems are described with guidelines coming from ISO standard for best practices in their implementation. Such best practices refer to the implementation of a number of governance components including:

- Open source software Policy;
- Open source software organisational committee;
- Open source software Risk Assessment (open source software risk register, open source software risk identification, measurement, evaluation, treatment, residual risks, …);
- Open source software Leadership;
- Open source software Supporting;
- Open source software Monitoring, measurement, analysis and evaluation;
- Open source software Internal Audit Plan;
- Open source software Management review;
- Open source software Incident Management system;
- Open source software Continual improvement.

5.2.2.2.2. External IT Support Management

Outsourcing management as described by the ISO 37500:2014 standard providing guidance on the following topics:

- Good outsourcing governance for the mutual benefit of client and provider;
- Flexibility of outsourcing arrangements, accommodating changing business requirements;
- Identifying risks involved with outsourcing;
- Enabling mutually beneficial collaborative relationships.

5.2.2.2.3. Internal IT Support Management

From the findings established in previous tasks of this study, training and internal open source software competence development could be further developed through activities including:

- Training;
- Collaborative platform to facilitate communication between stakeholders;
- Recruitment of experts;
- Handover to internal teams.

5.2.2.2.4. Quality management

Quality management is essential in any System Development Life Cycle (SDLC) and can be based on actions including:

- Quality code documentation;
- Code review;
- Penetration testing;
- Code auditing;
- Code crossed review;
- Reference to main security frameworks.

5.2.2.2.5. Identification of a maturity model and identified targeted level

When organising a competence centre like an open source software Development Team, it's important to measure the level of maturity of the team through an investigation on the core and supporting processes. The core processes being the ones that build and focus on the outputs, while the supporting processes being the ones that contribute to the facilitation of the core ones.

- Establishing a Capability Maturity Model for open source software code production;
- As-Is context;
- To-Be target;
- Action plan for moving to the To-Be (Target) maturity level.

5.2.2.2.6. Information and knowledge

Information and knowledge management is a necessary foundation to any team-related activity. It has also been mentioned in previous tasks as an essential need for any organisation having to manage internal or external activities relating to open source software development and production. Such activities include:

- Setting up a collaborative platform to allow communication between developers and stakeholders including:
  - Weblog;
  - Chat service;
  - Link with legal experts;
  - Project repository from design to operations;

- Definition of level of expertise, open source software -related functions, open source software job description.

5.2.2.2.7. Automated tools

Automated tools have been defined as findings in the previous tasks and it equally refers to best practices in IT (i.e. ITIL and ISO20000).

- Adopting automated tools to ease the checks on licencing compatibility;
- Automating activities as much as possible for all aspects relating to open source software activities management.

5.2.2.2.8. Monitoring tools

Monitoring tools should also be put in place in order to verify the delivered performance provided by the external leaders (i.e. the service providers).

- Monitoring of services under delivery process;
- Evaluation of delivered open source software services;
- Identification of a complaint process.

5.2.3. DOCUMENT REQUIREMENTS IN THE MANNER FOR FINAL INPUT TOWARDS A CALL FOR TENDERS

5.2.3.1. Table of requirements for tenders

Considering the fact that the European Commission will involve external providers to deliver services that will fulfil their requirements, it is important to ensure that such requirements are expressed in a S.M.A.R.T. way , namely :

1. Specific: written out clearly with concise goals
2. Measurable providing the ability to track the progress
3. Achievable set in a challenging mode, however with achievable goals
4. Relevant establishing goals that are relevant to the open source software project life plan
5. Time-based making sure that goal has a target finish time attached

The next table lists the requirements to be submitted to external providers with questions that clarify the position in relation with the requirement. Those requirements are reformulated to be more concretely understood by service providers and are ranged by categories. In practice at the time to launch the call for tenders, it will be necessary to add columns to be filled in by service providers in order to indicate their level of compliance with the requirement (Fully, Partially compliant, or No compliance).

CATEGORY	REQUIREMENTS	Questions to be addressed
Governance	➢ Open source software Policy; ➢ Open source software organisational committee; ➢ Open source software Risk Assessment (open	1. How do you organise the open source software Governance to manage the project that will be delivered in response of this request? 2. Does your current open source software Governance policy include all the necessary components such as: open source software Policy, open source software Risk Organisation Committee, open source software Risk Assessment, open source software Leadership, open source software

CATEGORY	REQUIREMENTS	Questions to be addressed
	source software risk register, open source software risk identification, measurement, evaluation, treatment, residual risks, …); ➢ Open source software Leadership; ➢ Open source software Supporting; ➢ Open source software Monitoring, measurement, analysis and evaluation; ➢ Open source software Internal Audit Plan; ➢ Open source software Management review; ➢ Open source software Incident Management system; ➢ Open source software Continual improvement.	Supporting, open source software Monitoring, open source software Internal Audit Plan, open source software Management Review, open source software Incident Management System? Please provide details about your answer. 3. In case of missing components in the current open source software Governance, what is your suggestion in order to fill these gaps and how will you apply alternative measures in the case of missing components? 4. How do you ensure the transfer of knowledge to European Commission so that the Governance can be implemented internally for the projects? 5. How and under which form will you introduce a mechanism of continuous improvement for the customer?
External IT Supporting Management	➢ Good outsourcing governance for the mutual benefit of client and provider; ➢ Flexibility of outsourcing arrangements, accommodating changing business requirements; ➢ Identifying risks involved with outsourcing; ➢ Enabling mutually beneficial collaborative relationships.	6. How do you handle and assign the ownership of: a. the supplied software (including all associated intellectual property rights with no restrictions on the purpose and type of use)? b. the source code (which may be studied by the public organisation or a third party for testing, training or other purposes)? c. the software which may be modified (by the public organisation or a third party in order to tailor it to its own needs)? d. and the software that can be distributed (with or without modifications by the public organisation to any party of its choice under the same terms and conditions)? 7. What is your approach regarding the management of IT Supporting activities? 8. Which clauses do you provide to ensure flexibility in the in terms of the outsourcing arrangements?

CATEGORY	REQUIREMENTS	Questions to be addressed
		9. How do you describe the IT supporting services in terms of time of intervention, volume of effort that you will deploy, and the level of service management? 10. How will you evaluate the customer satisfaction and pursue activities to ensure complete customer satisfaction?
Internal IT Supporting Management	➢ Training; ➢ Collaborative platform to facilitate communication between stakeholders; ➢ Recruitment of experts; ➢ Handover to internal teams.	11. How will you ensure having the appropriate experts to provide the required level of expertise and how will those experts interact with the internal developers? 12. Which activities do you foresee from your catalogue to improve the competence of internal developers at European Commission Software Development Team? 13. How will you organise the transfer of knowledge from your organisation to the Software Development Team? 14. Which tool (open source or otherwise) will you provide in the context of this project to support internal competence of developers? 15. How will you ensure the continued level of service in the event of people turn-over within your team?
Quality Management	➢ Quality code documentation; ➢ Code review; ➢ Penetration testing; ➢ Code auditing; ➢ Code crossed review; ➢ Reference to main security frameworks.	16. Which activities do you plan to include for quality improvement? 17. What do you foresee in terms of code documentation improvement, code review, and code crossed review? 18. How do you plan to include penetration testing, code auditing and inclusion of security measures allowing for improved compliance with internal security framework and associated internal policies? 19. How do you follow OWASP recommendations? 20. Which software do you use for code repository, testing, integration, security scanning, bug reporting and deployment?
Maturity Management	➢ Establishing a Capability Maturity Model for open source software code production; ➢ As-Is context; ➢ To-Be target; ➢ Action plan for moving to To-Be level.	21. How do you establish a capability maturity model and approach to analyse the AS-IS situation and establish a TO-BE target, both resulting in a Security Action Plan and Roadmap? 22. How do you plan to implement that model in the context of the project / services to be delivered? 23. How will you identify and formalise the gap between the AS-IS and TO-BE maturity levels? 24. Which services will you provide in order to support the previous point to fill the gap between the AS-IS and TO-BE maturity levels? 25. How will you share the maturity model framework and templates with the customer for reusability and future recurring maturity assessments internally?

CATEGORY	REQUIREMENTS	Questions to be addressed
Information and knowledge management	➢ Setting up a collaborative platform to allow communication between developers and stakeholders including: ▪ Weblog; ▪ Chat service; ▪ Link with legal experts; ▪ Project repository from design to operations; ➢ Definition of level of expertise, open source software -related functions, open source software job description.	26. What kind of collaborative platform do you provide to allow communication between developers and stakeholders? 27. Is that platform going to be implemented at the EC for use by the Software Development Team and free of charge to the EC or is there an associated cost? In case there is a cost, how is it included in your proposal? 28. How do you plan to implement that platform in the context of the open source software project / services to be delivered and under which conditions? Under which conditions will the platform stay in place for use by the customer after the project/contract has ended? 29. Which feature will be covered by that platform? 30. How would you ensure the security of that collaborative platform? Will it be located in Europe?
Automated tools management	➢ Adopting automated tools to ease the checks on licencing compatibility; ➢ Automating activities as much as possible for all aspects relating to open source software activities management.	31. Which automated tools are available from your current catalogue of automated tools? 32. Which ones will you implement or produce/develop in the context of this project / services? 33. How do you plan to implement those tools within the environment of the Software Development Team? 34. Will the tools stay in place for use by the customer after the end of the project/contract? 35. How secure will these tools be?
Monitoring tools management	➢ Monitoring of services under delivery process; ➢ Evaluation of delivered open source software services; ➢ Identification of a complain process.	36. Which monitoring tools can you provide from your current catalogue of automated tools? 37. Which ones will you produce or develop to be made available in the context of this project / services to be delivered? 38. How do you plan to implement these tools within the environment of the Software Development Team? 39. Will these tools stay in place for use by the customer after the end of the project/contract? 40. How secure will these tools be?

5.2.3.2. Additional considerations[27]

In the first instance, the Contractor recommends NOT to enforce definitive requirements in Call for Tenders, but rather to determine whether the service provider is currently compliant or not, and if not, whether they will become compliant by the end of the project or after a specific period of time. The period of time for compliancy would be defined in function of the context (i.e. project for development of an open source software application, maintenance service activity, bug fixing support, …).

In order to evaluate the compliance of the service provider with each submitted requirement, it will be important to ask the service providers to confirm their position as being:

1. **Fully compliant** (the customer will add an "X" in this column if they confirm full compliance with the specified requirement; they will also justify their choice by adding comments in the last column).
2. **Partially compliant** (the customer will indicate their percentage of compliance in this column in case of partial compliance; they will also justify their choice by adding comments in the last column as well as explaining how they will adapt themselves to cover the gap).
3. **No compliant** (the customer will add an "X" in this column if they are not compliant at all for this requirement; they will justify their position by adding comments in the last column as well as explaining how they suggest covering this requirement).
4. **Comments:** the customer will add comments in this column to clarify their position either by:
    - Providing evidence of full compliance;
    - Providing evidence of partial compliance and explaining optional suggestions for covering the non-compliant activities by compensation measures to reach a better level of compliance;
    - Justifying the non-compliant status with arguments for non-applicability or compensating measures.
5. In all cases, the service provider should be authorized to propose adding, modifying and/or cancelling a requirement by justifying or explaining their arguments for this change or deviation to the initial requirement. The European Commission will then analyse the comments of all the service providers in order to perform a lessons learned and investigate the possible adaptations of the requirements list:
    - Either by removing a requirement when such requirement would be systematically declined by all service providers, meaning that such a requirement is probably not acceptable or achievable and should then be considered for adaptation in its formulation or just be removed from the list.
    - Either by modifying the formulation of a requirement for which several service providers would suggest modifications and/or would indicate partial or no compliance.
    - Either by adding new requirements in the case that one or several service providers mentions a missing requirement.

Ideally, the Call for Tenders will also provide the possibility for Tender candidates to make suggestions and provide comments globally or specifically per requirement in the context of the Call for Tenders.

Many of the listed requirements can be considered as applicable not only to open source software IT Support aspects but also to proprietary software. Such results were also confirmed by other studies such as the one from the Turku

[27] In practice, when considering a specific "OSS services Call for Tenders", it will be convenient to address the formal requirements under the form of a worksheet table in which an additional column will indicate the relevance for the customer of each question (applicable or not) and other columns will be at the disposal of the service providers to express their level of compliance with regards to the requirement and will add descriptive explanation to illustrate his answer.

University in Finland[28] which mentions on page 78, that *"the main difference between a proprietary software license and an open source software license is that a proprietary license is aimed to secure the code for the developing organization itself, and open source license exists for securing the freedom of the code for everyone"*. Later at page 79 of the same document, it mentions that *"Empirical study shows, that none of the open source specific factors are important in open source projects. Instead the findings show that open source software should be managed just as a proprietary software business or any other type of business"*. The Turku paper ends with the following statement mentioning that *"In summary, the theory somewhat conflicts with the empirical findings as it seems that critical success factors in open source software projects are the same as in any other business model."*

5.2.4. DEFINING KEY SUCCESS FACTORS, METRICS AND MINIMUM CRITERIA TO HELP SET A BENCHMARK FOR FUTURE VENDOR SELECTION VIA A CALL FOR TENDERS

The section below builds upon the work in the requirements table presented in the previous section and adds the key success factors, metrics and minimum criteria with regard to the defined requirement categories.

Before presenting the new table mentioned above, some illustrations and references[29] published by the SMILE organization in the document "Points of view on open source, Analysis and decryption" illustrate the categories of requirements already identified previously:

- The importance in implementing an **open source software Governance** as a whole: an important aspect of open source software finding is to allocate sufficient importance to the setup of an open source software Governance Policy. As mentioned in the Smile reference[30], *"…open source has also brought a new approach to R&D. A good illustration is given by the open source project Genivi, which, at the initiative of BMW and PSA, brought together major car manufacturers and equipment manufacturers in a typical R&D approach pooled, building together a software platform for their vehicles. To succeed in this strategic project, these major industrialists have adopted the open source model both in terms of base, development, dissemination, and governance."*
- The importance to make a distinction between **internal** open source software expertise development and use of **external** outsourcing in function of the needs of the project and the expertise that's being required: both methods can be successfully used to provide the desired benefits and need to be considered in function of the presence of competent resources internally within the European Commission's Software Development Team and/or externally (i.e. with the service providers).
- The importance in understanding the concept of **Reusability** when developing new software: also, as mentioned in the Smile reference, *"Software development has also been profoundly changed. The modern approach to development involves assembling components, large and small, mostly open source. A decisive part of development therefore consists in selecting the right components and integrating them, by really developing only the specific parts, which concentrate the added value of the application. It is a transformation of software development that has brought significant productivity gains."*. Open source promotes the reusability of developed codes so that these can serve as modules to be used by other applications, instead of redeveloping as a whole.
- The importance to facilitate the **contracting procedure** in order to establish the right access with experts on the market: It is important to understand how to access open source software experts on the market. A publication[31] of Smile mentions that *"Open source publishers whose product does not have a global*

[28] See Master's Thesis in International Business by Erika Loimukallio, "Success factors of commercial open source software projects", 31/08/2012, Turun kauppakorkeakoulu, Turku School of Economics, pages 78 and 79.

[29] Smile, Points de vue sur l'Open Source, Analyses et décryptages, see internet : https://www.smile.eu/fr/publications/liste-livres-blancs, consulted on 20/01/2020.

[30] Ibid. p. 8

[31] Ibid. p. 13-14

deployment may have great difficulty in becoming profitable. Many are also integrators of their product. It is the easiest way to find revenue, at least to get started, and you would think that no one will be able to deploy a product better than the one who created it. But it is a model which is not extensible, and which tends to curb the expansion of the company. To deploy, especially internationally, the publisher must rely on a network of partner integrators, and it will never succeed in building this network if it is also the first competitor of its partners. Open source publisher-integrators therefore have a model that holds water, but which confines them to a small market. In a way, the product is there to help sell integration, the real source of income; he is only a competitive asset at the service of an integrator's core business."

- The importance of targeting **Quality and Maturity Management**, specifying the desired or committed level: The open source Software Development Team at DIGIT should be subject to a periodic evaluation in terms of Quality and Maturity Management. Such evaluation should include the measurement of the AS-IS maturity level together with a decision for a desired TO-BE maturity level. This target maturity level, once validated by the management, will ideally be accompanied by an action plan and a roadmap aiming to reach the target level within a given set period. Additional tools will be necessary including, for example, continuous monitoring of services to verify the level of quality achieved. For example, monitoring of services can include penetration testing, code reviews and audits, etc.

The next table revisits the Support requirements with the indication of possible Success Factors and Key Performance Indicators/Minimum Criteria in 3rd and 4th columns. It's to be noted that such information is indicative, to be used as a foundation before tailoring the list to the more accurate requirements of the European institutions, once the Go Ahead has been declared to launch a Call for Tenders.

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
Governance	➢ Open source software Policy; ➢ Open source software organisational committee; ➢ Open source software Risk Assessment (open source software risk register, open source software risk identification, measurement, evaluation, treatment, residual risks, …); ➢ Open source software Leadership; ➢ Open source software Supporting; ➢ Open source software Monitoring, measurement, analysis and evaluation; ➢ Open source software Internal Audit Plan; ➢ Open source software Management review; ➢ Open source software Incident Management system;	Provider has expertise, methodology and accompanying tools to implement all components of the open source software Governance.	Developed open source software Policy. Risk Assessment methodology implemented and applied to all applicable domains. Committed Budget and resources. Monitoring system. Internal Audit Plan and Program on a 3 years basis. OSRB components reviewed by the management. Implemented and operational Incident Management System. Implemented process for improvement.

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
	➢ Open source software Continual improvement.		
External IT Supporting Management	➢ Good outsourcing governance for the mutual benefit of client and provider; ➢ Flexibility of outsourcing arrangements, accommodating changing business requirements; ➢ Identifying risks involved with outsourcing; ➢ Enabling mutually beneficial collaborative relationships.	Identification of open source software services specifications for outsourcing. Identification of level of service required and performance. Monitoring of delivered services Renegotiation of outsourcing in function of deviation between performance specifications and delivery.	Coherence between the list of proposed and delivered services . Performance of delivered services in line with tolerance zone as contractually agreed. Existence of specific clauses in outsourcing contract for contract adaptation.
Internal IT Supporting Management	➢ Training; ➢ Collaborative platform to facilitate communication between stakeholders; ➢ Recruitment of experts; ➢ Handover to internal teams.	Existing and operational training catalogue. Implemented open source software collaborative platform. Built list of open source software expertise areas and internal needs Developed process for knowledge handover to internal staff.	Review on yearly basis of training needs based on open source software market evolution. Involvement of more than 80% of staff in the collaborative platform since last month. A good balance between the number of open source software experts and the project needs (in the critical path). Implemented process for knowledge handover to internal staff.
Quality Management	➢ Quality code documentation; ➢ Code review; ➢ Penetration testing; ➢ Code auditing; ➢ Code crossed review; ➢ Reference to main security frameworks.	Assigned open source software Quality Manager. Established quality code management process. 3 years based program for quality code review, code review, penetration	Date of last intervention is less than 6 months for: Quality code review Code review Penetration testing Code auditing Code crossed review

CATEGORY	REQUIREMENTS	SUCCESS FACTORS	KPIs / MINIMUM CRITERIA
		testing, code auditing, code crossed review.	
Maturity Management	➢ Establishing a Capability Maturity Model for open source software code production; ➢ As-Is context; ➢ To-Be target; ➢ Action plan for moving to To-Be level.	Established maturity model and defined as-is/to-be levels. Defined action plan for moving to To-Be level.	Scheduled action plan and updated status of rolled out actions
Information and knowledge management	➢ Setting up a collaborative platform to allow communication between developers and stakeholders including: ▪ Weblog; ▪ Chat service; ▪ Link with legal experts; ▪ Project repository from design to operations; ➢ Definition of level of expertise, open source software related functions, open source software job description.	Implemented collaborative platform with communication and coordination features for information knowledge management and coordination activities between open source software staff. Level of interaction of the developers with Communities	Operational collaborative platform and involvement of more than 80% staff during last 3 months. Recognized expertise as open source software developer in open source software Communities.
Automated tools management	➢ Adopting automated tools to ease the checks on licencing compatibility; ➢ Automating activities as much as possible for all aspects relating to open source software activities management.	Established list of needs for automated tools. Identified tools corresponding the needs.	Implemented tools and delivery of outputs on an adhoc basis.
Monitoring tools management	➢ Monitoring of services under delivery process; ➢ Evaluation of delivered open source software services; ➢ Identification of a complain process.	Identified list of monitoring needs. Selected monitoring tools corresponding to the needs.	Implemented monitoring tools 100% operationality

6. CONCLUSION OF THIS STUDY

The present study results with a list of formal requirements that service providers should address for each Call for Tenders when it relates to open source projects.

The study focused on two major aspects of open source:

1. The Requirements relating to Intellectual Property Rights and Licensing Support
2. The Requirements for Information Technology Support

These two topics were subject to information collection at each step of the Study:

1. Step 1, relating to Tasks 2 and 6: Identification of the needs of European institutions;
2. Step 2, relating to Tasks 3 and 7: Identification of the best practices adopted by a sample of selected service providers;
3. Step 3, relating to Tasks 4 and 8: Establishment of a Way Forward, under a list of recommendations through a number of selected best practices to fulfil the needs of European institutions;
4. Step 4, relating to Tasks 5 and 9: Elaboration of a list of Formal Requirements structured in eight categories. These formal requirements can be considered by European institutions for insertion in Call for Tenders at each time such a Call for Tenders will be published in the field of open source software.

The conclusion of this Study comes from the final 4th step which provides a list of 8 categories that regroups the findings by theme. The elaboration of these categories has been based on the list of findings that are presented in Appendix B.

The eight categories that have been defined at Step 4 are governance, external support management, internal support management, quality management, As-Is and To-Be maturity model, information and knowledge, automated tools and monitoring tools.

Appearing as the main results of this study, the following benefits have been provided to the European institutions, through the outputs coming out from the Step 4 of the study (Tasks 05 and 09):

1. The availability of a list of formal requirements that can be used by European institutions to be submitted to service providers at the time that a selection of service providers must be performed. Those requirements are accompanied by a list of questions as well as Key Success Factors, Metrics and Minimum Criteria to help set a benchmark for future vendor selection via a Call for Tenders,
2. The availability, in addition to the list of formal requirements, and by category, of a list of accompanying Key Success Factors, Metrics and Minimum Criteria that will help set a benchmark for future vendor selection via a Call for Tenders when such Call for Tenders is launched.

Beyond the here above mentioned benefits, it is worth to close this study with the following actual conclusions:

1. It is imperative to formally manage the open source software projects by adopting an appropriate governance;
2. The requirements for open source software projects are rather comparable to the requirements that would be established for proprietary software;
3. Open source software projects that would be insufficiently managed will inevitably bring new risks and introduce new security threats in the organisation;
4. The reason for introducing open source software in the organisation must be based on business drivers and business requirements. All maintenance, licensing and security activities should be selected in function of their contribution to the business objectives.

6.1. BIBLIOGRAPHY

6.1.1. Classic documents

1. HADDAD, Ibrahim. With contributions from COUGHLAN, Shane and STEWART, Kate. 2018. Open Source Compliance in the Enterprise. The Linux Foundation.
2. JEAN, Benjamin. 4th June 2019. *Seminar « Optimiser l'usage des logiciels libres et open source », second day*.
3. ROSEN, Lawrence. 2004. *Open Source Licensing: Software Freedom and Intellectual Property Law*. Upper Saddle River : Prentice Hall.

6.1.2. Electronic documents

1. ARMERDING, Taylor. 2019. *You're using open source software, and you need to keep track of it*. Available at: https://www.synopsys.com/blogs/software-security/track-open-source/, last consulted on the 24th January 2020.
2. AVERSANO, Lerina, Maria TORTORELLA. 2015. *Analysing the Reliability of Open Source Software Projects*. Available at: https://www.scitepress.org/papers/2015/55199/55199.pdf, last consulted on the 24th January 2020.
3. BRIDGWATER, Adrian. 2015. *The Seven Laws Of Open Source Leadership*. Available at: https://www.forbes.com/sites/adrianbridgwater/2015/09/06/the-seven-laws-of-open-source-leadership/#3aa5dd886ccf.
4. CIGREF. 2018. *L'Open Source, une alternative aux grands fournisseurs*. Available at: https://www.cigref.fr/wp/wp-content/uploads/2018/12/Cigref-Open-source-Alternative-Grands-Fournisseurs-franchir-pas-open-source-Decembre-2018.pdf, last consulted on the 24th January 2020.
5. ERNITS, Margus, Johannes TAMMEKÄND, Olaf MAENNEL. 2015. *i-tee: A fully automated Cyber Defense Competition for Students*. Available at: http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p113.pdf, last consulted on the 24th January 2020.
6. GUIMARD, Xavier. 2018. *La Politique des Logiciels de la Gendarmerie Nationale*. Available at : https://joinup.ec.europa.eu/sites/default/files/news/2018-07/20090305_noiv_jaarcongres_xavier_guimard_05032009.pdf, last consulted on the 24th January 2020.
7. JEAN, Benjamin, *Audit de licences : licences commerciales ou Open Source, un même combat ?*. Available at: https://www.journaldunet.com/solutions/expert/60469/audit-de-licences---licences-commerciales-ou-open-source--un-meme-combat.shtml, last consulted on the 24th January 2020.
8. LIU, Guan Ya. 2019. *3 factors for successful open source contributions*. Available at: https://developer.ibm.com/blogs/3-factors-for-successful-open-source-contributions/, last consulted on the 24th January 2020.
9. LOIMUKALLIO, Erika. 2012. *Success factors of commercial open source software projects*. Master's Thesis in International Business. Turun kauppakorkeakoulu, Turku School of Economics.
10. LUSZCZ, Jeff. 2017. *Artifex V. Hancom: Open Source Is Now An Enforceable Contract.* Available at: https://www.linux.com/tutorials/artifex-v-hancom-open-source-now-enforceable-contract/, last consulted on the 24th January 2020.
11. MEEKER, Heather. 2017. *Open source licensing: What every technologist should know*. Available at: https://opensource.com/article/17/9/open-source-licensing, last consulted on the 24th January 2020.
12. MILAN, Anthony. 2009. *Le logiciel libre en gendarmerie : 70% d'économie*. Available at: https://linuxfr.org/news/le-logiciel-libre-en-gendarmerie-70-d%C3%A9conomie, last consulted on the 24th January 2020.
13. RISKIN, Michael. 2018. *Is breach of the GPL license breach of contract?*. Available at: https://www.synopsys.com/blogs/software-security/breach-gpl-license-breach-contract/, last consulted on the 24th January 2020.

14. SMILE. *Understanding open source and free software*, Available at: https://www.smile.eu/en/publications/list-white-papers.
15. STALLMAN, Richard M. 2006. *Don't Let 'Intellectual Property' Twist Your Ethos*. Available at: https://www.gnu.org/philosophy/no-ip-ethos.html, last consulted on the 24th January 2020.
16. SYNOPSYS EDITORIAL TEAM, 2019. *Top open source licenses and legal risk for developers*. Available at: https://www.synopsys.com/blogs/software-security/top-open-source-licenses/, last consulted on the 24th January 2020.

6.1.3. Document from the European institutions

1. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Against lock-in: building open ICT systems by making better use of standards in public Procurement [COM(2013) 455 final]

6.1.4. Websites

1. https://elastest.eu/project.html, last consulted on the 24th January 2020.
2. https://eupl.eu/, last consulted on the 24th January 2020.
3. https://feb.kuleuven.be/public/u0003131/Matrices/GNU%20License.htm, last consulted on the 24th January 2020.
4. https://euipo.europa.eu/ohimportal/fr/home, last consulted on the 24th January 2020.
5. https://en.wikipedia.org/wiki/Patch_(computing)#In_software_development, last consulted on the 24th January 2020.
6. https://euipo.europa.eu/, last consulted on the 24th January 2020.
7. http://oss.management/, last consulted on the 24th January 2020.
8. https://opensource.org/licenses, last consulted on the 24th January 2020.
9. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.7299&rep=rep1&type=pdf, last consulted on the 15th November 2019.
10. https://www.inria.fr/, last consulted on the 24th January 2020.
11. https://fr.wikipedia.org/wiki/Licence_CeCILL, last consulted on the 24th January 2020.
12. https://uclouvain.be/en/research/ltto, last consulted on the 24th January 2020.
13. https://uclouvain.be/en/research/ltto/mission-and-team.html, last consulted on the 24th January 2020.
14. https://www.inria.fr/en/centre/saclay/innovation/technology-assets/software, last consulted on the 15th November 2019.
15. https://medinsoft.com/commission/commission-logiciel-libre/, last consulted on the 24th January 2020.
16. https://www.linuxfoundation.org/about/, last consulted on the 24th January 2020.
17. https://todogroup.org/guides/management-tools/, last consulted on the 24th January 2020.
18. https://choosealicense.com/, last consulted on the 24th January 2020.
19. https://fossa.com/, last consulted on the 24th January 2020.
20. https://inno3.fr/services/audit-conformite, last consulted on the 24th January 2020.
21. https://www.gnu.org/licenses/agpl-3.0-standalone.html, last consulted on the 24th January 2020.
22. https://joinup.ec.europa.eu/collection/oslo-open-standards-local-administrations-flanders/about
23. https://biblio.ugent.be/publication/8504205/file/8504206, last consulted on the 15th November 2019.
24. https://opensource.dell.com/, last consulted on the 24th January 2020.
25. https://www.ibm.com/fr-fr/cloud/redhat, last consulted on the 24th January 2020.
26. https://www.ibm.com/services/technology-support/open-source, last consulted on the 24th January 2020.
27. https://www.ibm.com/support/customer/csol/soweb/pdf/archive/sow/ch-en/bupa/sowsupportlinebp.pdf, last consulted on the 24th January 2020.
28. https://www.blackducksoftware.com/, last consulted on the 24th January 2020.
29. http://www.eenet.ee/EENet/EENet_en, last consulted on the 24th January 2020.
30. https://linux.slashdot.org/story/18/01/15/0415219/city-of-barcelona-dumps-windows-for-linux-and-open-source-software, last consulted on the 24th January 2020.

31. http://www.ososs.nl/, last consulted on the 24th January 2020.
32. https://www.softwareheritage.org/, last consulted on the 24th January 2020.
33. https://www.softwareheritage.org/2019/09/05/software-heritage-for-open-science/?lang=fr, last consulted on the 24th January 2020.
34. https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF, last consulted on the 24th January 2020.
35. https://ec.europa.eu/isa2/solutions/eira_en, last consulted on the 24th January 2020.
36. https://www.gnu.org/proprietary/, last consulted on the 24th January 2020.
37. https://www.gnu.org/proprietary/malware-microsoft.html, last consulted on the 24th January 2020.
38. https://github.com/magavdraakon/i-tee, last consulted on the 24th January 2020.
39. https://rangeforce.com/home, last consulted on the 15th November 2019.
40. https://jitsi.org/jitsi-meet/, last consulted on the 24th January 2020.
41. https://alternativeto.net/software/jitsi-meet/?license=opensource, last consulted on the 24th January 2020.
42. https://fr.wikipedia.org/wiki/Linagora, last consulted on the 24th January 2020.
43. https://fr.wikipedia.org/wiki/Smile_(entreprise) , last consulted on the 24th January 2020.
44. https://developer.ibm.com/open/, last consulted on the 24th January 2020.
45. https://wso2.com/about/, last consulted on the 24th January 2020.
46. https://en.wikipedia.org/wiki/Bechtle, last consulted on the 24th January 2020.
47. https://en.wikipedia.org/wiki/Red_Hat, last consulted on the 24th January 2020.
48. https://blog.bosch-si.com/bosch-iot-suite/the-benefits-of-open-source/, last consulted on the 24th January 2020.

7. APPENDIX A: LIST OF OPEN SOURCE SOFTWARE ASSETS USED BY EUROPEAN INSTITUTIONS AND NON-EC OPEN SOURCE SOFTWARE LEADERS INTERVIEWED

The table below is supplied as a reference of the software, languages, solutions, practices and tools cited during the interviews or in the questionnaire replies. This list should not be considered as exhaustive.

Assets (1/4)			Gendarmerie Nationale Française	DGFiP	UCLouvain	Alter Way	Libertis	Alvatal	European Commission	European Parliament	European council
Authentication	Web SSO		X								
Servers	Linux			X	X						
	J2EE Jboss			X							
	Tomcat (java web)			X						X	
	Jenkins				X						
	IMAP (mails)			X							
	Git									X	
Operating system	Linux									X	
	Fedora (GNU/Linux)									X	
	Ubuntu (Linux)		X								
Web Browsers	Mozilla Firefox		X		X				X		
	Open Journal Systems (OJS)				X						
	Safe Exam Browser (SEB)				X						
Platforms	GitLab				X						
	Java									X	
	ElasTest (testing)								X		
	Umbraco (CMS)										X
	Alfresco (CMS)										X
Development kits	Java Development Kit (JDK)			X							
Development platforms	Jenkins									X	
	Nexus									X	
Frameworks	Java Spring									X	
	ACube										X
	.NET Core										X
	Symfoni (php)								X		
	Java Angular								X		

Assets (2/4)			Gendarmerie Nationale Française	DGFiP	UCLouvain	Alter Way	Libertis	Alvatal	European Commission	European Parliament	European council
Web Frameworks	Django						X				
Package Management tool	Maven									X	
Applications/Software	CMS					X					
	Drupal (CRM)				X	X			X		
	DSpace (repository)				X						
	Scilab				X						
	Moodle				X						
	Thunderbird (mails)			X							
	Doodle				X						
	DroneCode								X		
	Matomo								X	X	
	IAST (security tests)								X		
	RASP (signals)								X		
	Splash (video-mapping)									X	
	Workplace solutions								X		
	Tomcat (web container)										X
	Mobile Apps (for Android & Apple Store)										X
Languages	Java		X	X					X		X
	R (for statistics)				X						
	Python						X				
	Slap				X						
	M			X							
	Pseudo-C			X							
Libraries	Google libraries										X
Databases	PostgreSQL			X							
	MySQL								X		
	Redis (DB cache)								X		
Database Libraries	Hibernate (with patterns)									X	
Wiki software/tools										X	

Assets (3/4)			Gendarmerie Nationale Française	DGFiP	UCLouvain	Alter Way	Libertis	Alvatal	European Commission	European Parliament	European Council
Linux workstations				X[32]						X	
Office tools/Text editors	Open Office		X					X			
	Slap				X						
Clouds	Azure (solution hybride)					X					
	Cloud with Open Source Software										X
Support & Maintenance services	Linagora	Maintenance		X							
		Audits	X								
	ANSSI	Audits (on iconic applications)		X							
Foundations / Products / Best practices	Apache			X		X				X	
	Linux					X			X		X
	Eclipse			X		X					
	Red Hat								X	X	X
	Mozilla								X		
	Joinup								X		
	Adobe								X		
	Docker								X		
	GitHub								X		
	Debian								X		
Communities / Projects	Tikal								X		
	OWASP (security)								X		X

[32] The Direction générale des Finances publiques (in France) is currently experiencing the introduction of workstations that are entirely running under Linux. This experience is concerning about one hundred workstations for the moment.

Assets (4/4)			Gendarmerie Nationale Française	DGFiP	UCLouvain	Alter Way	Libertis	Alvatal	European Commission	European Parliament	European council
References supplied:											
Platform virtualization software	VirtualBox							X			
Virtual laboratory	i-Tee[34] (on GitHub)							X			
Cybersecurity training platform	rangeforce[35]							X			
Free video conferencing	Jitsi[36]							X			
Free Software Foundation Project/Operating system GNU[33]								X			

[33] https://www.gnu.org/proprietary/
https://www.gnu.org/proprietary/malware-microsoft.html

[34] http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p113.pdf
https://github.com/magavdraakon/i-tee

[35] https://rangeforce.com/home

[36] https://jitsi.org/jitsi-meet/
https://alternativeto.net/software/jitsi-meet/?license=opensource

8. APPENDIX B LIST OF FINDINGS

The table below lists the findings as identified through tasks 2, 3, 6 and 7. The table adds a reference number to each finding (# number) which is used in section 4 to map the recommendations with the findings established through the study.

#	Task #	Finding
1	2	Reaching deeper knowledge of the risks related to licencing aspects in the use of open source software solutions.
2	2	Informing development teams about Legal support and copyright expertise within EC.
3	2	Developing corporate policy for using, integrating, developing open source software and managing licencing issues.
4	2	Establishing a framework for reusability of open source software tools (ISA 2020).
5	2	Adapting procurement framework to allow access to small open source software providers.
6	2	Establishing policy and guidelines for contribution to communities.
7	2	Providing advice on choice of licences and procedure for licences verification by legal teams.
8	2	Supporting consolidation of open source software and licence catalogues.
9	2	Adopting automated tools to ease the checks on licence compatibility.
10	2	Achieving better mutualisation of tools within EC & EU institutions.
11	3	Ensuring better awareness about open source software in the field of IPR.
12	3	Taking into account the potential adverse consequences of non-compliance.
13	3	Managing licensing aspects of open source software.
14	3	Improving the communication between all stakeholders.
15	3	Organising trainings for all people consuming open source components.
16	3	Implementing tools to track licences in open source components
17	6	EC institutions to increase guarantee in relation with support & maintenance activities.
18	6	Support relating to corrective maintenance activities (bugs fixing).
19	6	EC institutions to establish a coherent vision for the 3 main European institutions i.e. Commission, Parliament and Council.
20	6	Further investigation about the reusability of open source solutions by other European entities.
21	6	A better communication about the available solutions that could fit the needs of every other one.
22	6	A better connection structure with the legal team to address the licencing issues.
23	6	Setting up incident management systems to deal with bugs.
24	7	Ensuring access to the right expertise to solve bugs and problems when they occur.
25	7	Considering smooth transition when moving from proprietary to open source software solutions.
26	7	Investing in human resources (internal open source software experts) to ensure adequate management of open source software projects (based on both internal developments and external solutions providers).
27	7	Establishing central decision when contracting maintenance services with external providers.

28	7	Assessing interoperability issues and coexistence of open source and proprietary products.
29	7	Investing in appropriate incident management system and procedures for bug fixing and problems solving.
30	7	Building cooperative platforms in order to achieve common objectives.