Subject: Your applications for access to documents


Dear Madam,

We refer to the request for access to documents which you made on 27 October 2017, which was registered on 6 November 2017 under the above-mentioned reference.

Your application is the following:


This includes emails, documents, notes, drafts, files, tables and other information. I want to have all information included, regardless whether it is considered short-lived or unimportant by the Commission."

First of all, we thank you for your request and your interest in the work of DG DIGIT in the field of open source software.

1. **Object of your request**

WP 4 is a work package (study) that has been requested within the framework of the Pilot Project "Governance and quality of software code – Auditing of free and open source software" (reference 26 03 77 02). This Pilot project has been split into several work packages (1 – 7) and a contractor has been requested to perform the study.

You specify that the answer to your request should: "include[f] emails, documents, notes, drafts, files, tables and other information. I want to have all information included, regardless whether it is considered short-lived or unimportant by the Commission".

First, we remind you that Regulation 1049/2001 only covers the access to document and must be clearly distinguished from the access to **information**¹ (see the bold part of your request in the previous paragraph). Access to information is subject by the specific rules laid down in the Code of Good Administrative Behaviour².

Also, in its decision of 23 January 2002 amending its Rules of Procedure (2002/47/EC, ECSC, Euratom), the Commission added an annex to the Rules of procedure. According to article 4 of this annex, "A document drawn up or received by a Commission department must be registered if it contains important information which is not short-lived and/or may involve action or follow-up by the Commission or one of its departments". The Commission is therefore not in a position to deliver documents "considered short-lived or unimportant" (see the underlined part of your request in the second paragraph of the present section).

Finally, and linked to the previous paragraph, the Commission can only grant access to the documents that have been properly stored and are therefore still in its possession: "Es ist darauf hinzuweisen, dass die Verordnung Nr. 1049/2001 zwar selbst dann anwendbar ist, wenn – wie die Kommission hier geltend macht – das betreffende Organ nicht mehr über das Dokument verfügt, zu dem Zugang verlangt wird, und dieses Organ dem Antragsteller antworten und vor Gericht die aus diesem Grund erfolgende Verweigerung des Zugangs rechtfertigen muss, doch kann diese Verordnung ein Organ nicht verpflichten, Zugang zu einem Dokument zu gewähren, über das es nicht mehr verfügt (vgl. in diesem Sinne und entsprechend Urteil Strack/Kommission, oben in Rn. 36 angeführt, EU:C:2014:2250, Rn. 38 bis 47)".³ (Judgment of the General Court of 26 April 2016 in case T-221/08, Strack v Commission).

The Commission has currently located that the documents in its possession regarding the Work Package 4 (WP 4) are stored on 3 different locations:

1. The U drive of the unit in charge of the EU-FOSSA project
2. The Advanced record system (Ares)
3. The communication tool used by the contractor to store the documents related to the EU-FOSSA project (the "Wiki")

³ This decision is only available in French and German, no English version is available. Taking into account your postal address, we provide you with an abstract of the German version.
The documents that have been identified as falling under the scope of your request are listed in Annex 1 of the present letter. Each document that has been identified has been numbered in the file; this number will be used to make reference to each specific document in the present letter.

Please also note that information regarding the Pilot Project "Governance and quality of software code – Auditing of free and open source software" (reference 26 03 77 02) has already been publicly released under the following link:

https://joinup.cc.europa.eu/page/project-deliveries

2. HOLDING LETTER

Due to the very large amount of documents targeted by the request (see Annex 1), we will not be in a position to complete the handling of your application within the time limit of 15 working days, which expires on 27 November 2017, and analyse all the documents contained in the wiki by then.

An extended time limit will in any event be required to grant you access to the largest amount of documents possible.

Therefore, we have to extend the time limit with 15 working days in accordance with Article 7(3) of Regulation (EC) No 1049/2001 regarding public access to documents.

The new time limit expires on 18 December 2017.

3. FAIR SOLUTION

3.1. Justification

Moreover, the Wiki contains a very large amount of documents and some of them are very long documents, that require to be scrutinised line by line in order to determine whether they contain (or not) security-related elements, personal data or any other elements that would fall within the exceptions of Article 4 of the Regulation 1049/2001.

In order to demonstrate our good faith, we already grant you access to certain documents that may obviously be released (see below).

However, the assessment of the remaining document will imply a very detailed analysis (and a very large amount of work) that cannot be carried out within the normal time limits set out in Article 7 of Regulation 1049/2001.

Article 6(3) provides that in the event of an application relating to a very long document or to very large number of documents, the institution concerned may confer with the applicant informally, with a view to finding a fair solution.

In accordance with the case law of the EU Courts, such a solution can only concern the content or the number of documents applied for, not the deadline for replying. This

---

means that the scope of the request must be reduced in a way that would enable its treatment within the extended deadline of 15 + 15 working days.

We are not in a position to assess which documents would really be of interest for you and we do not want to privilege the analysis of certain documents while you might actually have interest in some other documents.

Therefore, based on the above-mentioned provision, we would kindly ask you to specify the objective of your request and your specific interest in the documents requested\(^5\), and whether you could narrow down the scope of your request (i.e. the subject matter(s) and/or timeframe covered), so as to reduce it to a more manageable amount of documents.

3.2. List of documents and documents to facilitate the identification of the objectives and specific interests of your request

In order to facilitate the precision of your request, the documents contained in the wiki and falling under the scope of your request have been fully listed in Annex 1. An indication of their length and, where possible, a description of their content has also been provided.

Also, in order to help you to narrow down your request, as these documents clearly fall under the scope of Article 2 of Regulation (EC) No 1049/2001, full access to the summary and presentation of the main deliverables of WP 4 is already granted to you. A copy of documents 25, 26 and 27 will be enclosed to the present letter.

We also invite you to take into consideration while narrowing down your request, should you decide to have one, that the documents, for which the column "status" is marked in blue in the Annex 1, are most likely to be partially or fully redacted for public security reasons (Article 4(1)(b) first indent of the Regulation 1049/2001 – see Section 6.2 of the present letter).

3.3. Proposition

In order to enable us to respect the time-limits of Regulation 1049/2001, we would ask you for a swift reply to our invitation to propose a fair solution, within five working days at the latest:

- by email to: DIGIT-ACCESS-TO-DOCUMENTS@ec.europa.eu
- by postal mail to: Commission européenne/Europese Commissie, rue Montoyer 15 1049 Bruxelles/Brussel, BELGIQUE/BELGIË Office: MO15 07/P001

If you have any questions concerning the invitation, you can contact us:

- by email at: DIGIT-ACCESS-TO-DOCUMENTS@ec.europa.eu
- by telephone at: (+32) (0) 229-52544

\(^{5}\)Ibid, paragraph 28; Judgment of the General Court (then 'Court of First Instance') of 22 May 2012 in case T-344/08, EnBW Energie Baden-Württemberg v Commission, paragraph 105.
We would also be available to schedule a conference call in a short timeframe to discuss your objectives and specific interests in this request and help you narrow down your request.

In the absence of reply from your side within five working days, and in order to balance the right to access to document and the good use of resources of the European Commission, we will restrict the scope of your application to those parts that can be dealt with within the extended deadline of 30 working days, counting from the registration of your application on 5 November 2017 and ending on 18 December 2017. We would then focus on the documents 6 to 28 and 38 to 49.

4. THE DOCUMENTS TO WHICH ACCESS MAY OBLIGEY BE GRANTED

4.1. Full Access

Pursuant to Article 2 of Regulation (EC) No 1049/2001, in addition to the documents listed in Section 3.2, full access to the documents 1, 2 and 12 has been granted to you fully and we enclose a copy of these requested documents.

A copy of these documents will be enclosed to the present letter. In order for you to easily identify these documents, the column "status" of these documents is marked in green. Please note that documents 2 and 12 have the same content, it will therefore only be provided once.

5. EXCEPTION ON PRIVACY AND INTEGRITY OF THE INDIVIDUAL (ARTICLE 4(1)(B) OF REGULATION 1049/2001)

5.1. Rules

As indicated in Annex 1, many documents contain personal information / data whose disclosure could undermine the protection of privacy and the integrity of the individual (see the documents for which the column "Name of the document" is marked in yellow).

Pursuant to Article 4(1)(b) of Regulation 1049/2001, access to a document has to be refused if its disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data. The applicable legislation in this field is Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

When access is requested to documents containing personal data, Regulation (EC) No 45/2001 becomes fully applicable.

According to Article 8(b) of this Regulation, personal data shall only be transferred to recipients if they establish the necessity of having the data transferred to them and if there is no reason to assume that the legitimate rights of the persons concerned might be prejudiced.

We consider that, with the information available, the necessity of disclosing the aforementioned personal data to you has not been established and/or that it cannot be
assumed that such disclosure would not prejudice the legitimate rights of the persons concerned.\(^6\)

5.2. Partial access due to the presence of personal data

According to Article 4(6) of Regulation 1049/2001, "If only parts of the requested document are covered by any of the exceptions, the remaining parts of the document shall be released". This article applies if only some parts of documents would contain personal data.

The Advanced record system of the Commission (Ares) contains one document regarding the WP 4: document 5. Access to this document may obviously be already granted to you. Partial access to this document has been granted to you. However, as it contains personal data, according to the Rules on Privacy, all personal information contained in the document will be redacted.

A redacted copy of this document is enclosed to the present letter.

5.3. Access likely to be fully denied due to the presence of personal data

Some of the documents falling under the scope of the request are solely a list of names (and contact details) and a list of curriculum vitae. These documents solely contain personal data.

The Commission is therefore likely to decide that access to these documents will be fully denied. In order for you to easily identify these documents, the column "status" of these documents is marked in red. This decision will occur in due course.

6. Access likely to be fully or partially denied due to other exception

6.1. Exception: Commercially sensitive business information

Access to some documents, including document 3, could be restricted in the way that some part of the document might need to be redacted.

As already pointed out, according to Article 4(6) of Regulation 1049/2001, if only parts of a document is covered by an exception, the specific part(s) will be redacted and the rest of the document will be release, this applies also for the exception: Commercially sensitive business information.

Regarding document 3 for example, pages 32 and 33 of document 3 contain commercially sensitive business information of the company that submitted the document. Indeed, it contains the prices that the company charges for the services specifically requested. The prices charged by a company for its products / services are generally regarded as commercially sensitive business information\(^7\). According to Article 4(2), first

---

\(^6\) In this letter, the rules described in this section will be hereafter referred to as "the Rules on Privacy (Article 8(b) of Regulation 1049/2001)".

indent of Regulation 1049/2001, it is highly likely that access to such commercially sensitive information may not be granted to you.

Therefore, it is most likely that the sensitive business information contained in the documents, and more specifically in pages 32 and 33 of document 3\(^8\) will be redacted before the document can be released.

6.2. Exception: public security

Having been through the documents contained in the Wiki, we have noted that it is likely that some (parts of the) documents are likely to fall under the public security exception such as provided in Article 4(1)(a) first indent. This exception is applicable if the disclosure of the document would put at risk the security of the EU.

Case law has specified that "The concept could equally well encompass situations in which public access to particular documents could obstruct the attempts of authorities to prevent criminal activities"\(^9\). Also, measures taken to protect the IT infrastructure of the EU should be kept out of the public domain as their disclosure would undermine the effect of the protection.

This being said, the publication of information (contained in documents) - concerning the IP address of Commission's computers, its IT infrastructure and the specific programmes and application installed on specific computers or used to protect it - could to enhance the security threat that could target the EU IT infrastructure and make such infrastructure more vulnerable toward hacking and threats.

Therefore, it is likely that publication of this specific information is likely to be covered by the exception on public security and that all (parts of) documents that would include it would require a specific redaction.

7. FINAL DISPOSITION

You may reuse the documents, to which access has been granted to you, free of charge for non-commercial and commercial purposes provided that the source is acknowledged, and that you do not distort the original meaning or message of the documents. Please note that the Commission does not assume liability stemming from the reuse.

The final assessment of the Commission, regarding the (partial or full) access or the denial of such access for the remaining documents listed in Annex 1, will be communicated to you in due course and on 18 December 2017 at the latest.

---

\(^8\) If document 3 is finally released, in addition, as pages 2 and 28 contain personal data that, according to the Rules on Privacy (Article 8(b) of Regulation 1049/2001), these will need to be redacted before release.

Enclosures:

1. Annex 1: List of documents covered by the request
2. Document 1: ABC technical annex WP3-5.docx
5. Document 25: DLV7 - WP4 Executive Summary
6. Document 26: DLV7 - WP4 Presentation
7. Document 27: DLV7 - WP4 Flyer leaflet version

Yours faithfully,

[Signature]

Martin BILBAO
Head of Unit
<table>
<thead>
<tr>
<th>Location</th>
<th>Folder</th>
<th>Subfolder</th>
<th>Subfolder</th>
<th>Name of the document</th>
<th>Description of the document (if necessary)</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>U: Drive</td>
<td></td>
<td></td>
<td></td>
<td>ABC technical annex WP3-5.docx</td>
<td>Technical Annex describing the work to be executed (text editing file format)</td>
<td>4 pages</td>
<td>Full Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ABC technical annex WP3-5.pdf</td>
<td>Technical Annex describing the work to be executed (printing file format)</td>
<td>4 pages</td>
<td>Full Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>offer_KonSult_1_Main.pdf</td>
<td>Offer of the consortium KonSult - main part</td>
<td></td>
<td>Access likely to be partially granted - Redaction of personal data and likely redaction due to the presence of commercially sensitive business information</td>
</tr>
<tr>
<td>Ares</td>
<td></td>
<td></td>
<td></td>
<td>offer_KonSult_2_CVs.pdf</td>
<td>Offer of the consortium KonSult - list of CVs</td>
<td></td>
<td>Access likely to be fully denied as it only contains personal data</td>
</tr>
<tr>
<td></td>
<td>Ares(2016)6600235</td>
<td></td>
<td></td>
<td>EP Pilot Project 645 - FOSSA WP3-5 - Deletion of confidential information</td>
<td>Confirmation of deletion of confidential information by the consortium after the project completion.</td>
<td></td>
<td>Access partially granted - Redaction of personal data</td>
</tr>
<tr>
<td>Wiki</td>
<td></td>
<td></td>
<td></td>
<td>FOSSA - Follow-up Report 15 06 2015.doc</td>
<td>Progress report</td>
<td>5 pages</td>
<td>Fair solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FOSSA - Follow-up Report 26 06 2015.doc</td>
<td>Progress report</td>
<td>5 pages</td>
<td>Fair solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Project Charter FOSSA 1.0.doc</td>
<td>Project Charter</td>
<td>24 pages</td>
<td>Fair solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Project Charter FOSSA 1 4.docx</td>
<td>Project Charter</td>
<td>23 pages</td>
<td>Fair solution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Project Charter FOSSA 1 4.pdf</td>
<td>Project Charter</td>
<td>23 pages</td>
<td>Fair solution</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>FOSSA WP345 Kick-off meeting presentation</td>
<td>Presentation for a Kick-off meeting: WP3-5</td>
<td>25 slides</td>
<td>Fair solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>FOSSA WP3-5 Task List</td>
<td>Task list: WP3-5</td>
<td>90 rows</td>
<td>Fair solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>FOSSA WP3-5 Issue Log</td>
<td>Issue log: WP3-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>FOSSA WP3-5 Risk Registry</td>
<td>Risk Registry: WP3-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>Meeting minutes (3-5)</td>
<td>Meeting minutes - Alignment of work packages WP4-5 and WP6</td>
<td>2 pages</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>WP3-5 Kick-off</td>
<td>Kick-off meeting minutes: WP3-5</td>
<td>3 pages</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>10 - Project progress reports (3-5)</td>
<td>FOSSA_WP345_Project_Progress_Report.docx</td>
<td>Progress report: WP3-5</td>
<td>10 pages</td>
<td>Fair solution</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Deliverables</td>
<td>DLV7 - WP4 Executive Summary</td>
<td>Dissemination materials for WP4</td>
<td>3 pages</td>
<td>Full Access</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td>DLV7 - WP4 Presentation</td>
<td>Dissemination materials for WP4</td>
<td>7 pages</td>
<td>Full Access</td>
<td></td>
</tr>
<tr>
<td>Page</td>
<td>Document Title</td>
<td>Description</td>
<td>Pages</td>
<td>Level of Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
<td>-----------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>DLV6 - Software Inventory</td>
<td>The main deliverable of WP4.</td>
<td>26 pages</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>DLV6 - Annex 1 - Inventory Summary</td>
<td>Inventory summary: total numbers of items and instances in scope, summary numbers of OSS instances.</td>
<td>28 rows of a summary table</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>DLV6 - Annex 2 - list of all software with instances</td>
<td>The complete list of all software installed at the EC with number of instances</td>
<td>46244 rows + 29615 rows</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>DLV6 - Annex 3 - List of OSS with instances</td>
<td>The list of OSS installed at the EC with number of instances</td>
<td>8227 rows</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>DLV6 - Annex 4 - OSS by system type</td>
<td>The list of OSS installed at the EC with number of instances, including system type (Workstation, Server, AppV)</td>
<td>8225 rows</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>DLV6 - Annex 5 - Proprietary software by system type</td>
<td>List of proprietary software installed at the EC with number of instances, including system type</td>
<td>37991 rows</td>
<td>Partially redacted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DLV6 - Annex 6 - OSS by Software Type</td>
<td>List of OSS by type of software</td>
<td>4515 rows + 2 charts and a summary table</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data and could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td>DLV6 - Annex 7 - List of critical OSS with rating</td>
<td>List of shortlisted critical OSS and its rating against criticality and sustainability criteria defined in WP1-2</td>
<td>829 rows</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data and could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td></td>
<td>DLV6 - Annex 8 - Software dependencies</td>
<td>Analysis of dependencies of the shortlisted OSS</td>
<td>105 + 68 rows and a chart</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data and could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td>DLV6 - Annex 9 - Elaborations on raw inventory data</td>
<td>Elaborations on raw inventory data for Top-30 items by software type (methods used to group the software for the top 30 list)</td>
<td>92 cells</td>
<td>Fair solution - Document likely to be at least partially redacted as it contains personal data and could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td></td>
<td>other outputs</td>
<td></td>
<td></td>
<td>Fair solution - Document likely to be at least partially redacted as it could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td></td>
<td>Docker environment for inventory</td>
<td>Documentation of the instance used for running the inventory.</td>
<td>3 pages</td>
<td>Fair solution - Document likely to be at least partially redacted as it could be covered by the exception on public security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td></td>
<td>FOSSA Inventory environment documentation</td>
<td>Documentation of the instance used for running the inventory.</td>
<td>4 pages</td>
<td>Fair solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>Pentaho dashboard creation guidelines</td>
<td>Documentation of the instance used for running the inventory.</td>
<td>3 pages</td>
<td>Fair solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Steering Committees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Page</td>
<td>Document ID</td>
<td>Title</td>
<td>Format</td>
<td>Pages</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-------</td>
<td>--------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>SC226 FOSSA M4_SteeringCommittee_Meeting_minutes 18-04-2016</td>
<td>Minutes of a Steering Committee</td>
<td>4 pages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>SC226 FOSSA M7_SteeringCommittee_Meeting_minutes, 11-07-2016</td>
<td>Minutes of a Steering Committee</td>
<td>3 pages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>SC226 FOSSA M10_SteeringCommittee_Meeting_minutes, 25-10-2016</td>
<td>Minutes of a Steering Committee</td>
<td>4 pages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>EU-FOSSA - Steering Committee 20161025 agenda</td>
<td>Agenda of a Steering Committee</td>
<td>1 page</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>EU-FOSSA - Steering Committee 20161025 presentation - part1</td>
<td>Presentation for a Steering Committee</td>
<td>14 slides</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>EU-FOSSA - Steering Committee 20160711 agenda</td>
<td>Agenda of a Steering Committee</td>
<td>1 page</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>EU-FOSSA Steering Committee 20160711 Presentation</td>
<td>Presentation for a Steering Committee</td>
<td>11 slides</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>EU-FOSSA - Steering Committee 20160408 agenda</td>
<td>Agenda of a Steering Committee</td>
<td>1 page</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>EU-FOSSA - Steering Committee 20160418 presentation</td>
<td>Presentation for a Steering Committee</td>
<td>14 slides</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TECHNICAL ANNEX – FOSSA WP3-5

1. CONTEXT / INTRODUCTION

This work is requested in the context of the Pilot Project "Governance and quality of software code – Auditing of free and open source software" (reference 26 03 77 02).

Recent discoveries of vulnerabilities in critical information infrastructure have drawn the broader public's attention to the need to understand how governance and quality of the underlying software code relates to basic safety and public trust in applications that are used on a day-to-day basis. As both the general public and the EU institutions regularly use free and open-source software - from end-user device applications to server systems - the need for coordinated efforts to ensure and maintain the integrity and security of that software has been highlighted by the European Parliament itself. This pilot project will offer a systematic approach to achieving a goal to which the EU institutions themselves can contribute, namely ensuring that widely used critical software can be trusted.

The project has been split into several work packages. This Technical Annex concerns Work Packages 3, 4 and 5 – preparation of a unified inventory methodology together with the necessary tools and preparation of inventories of free and open source software and open technical specifications used by the European Commission and the European Parliament.

2. DESCRIPTION OF TASKS

The contractor will perform the following tasks:

Work Package 3

Task 1: Development of a methodology to perform periodic inter-institutional inventories of software assets and standards

The contractor will collect the European Commission's and European Parliament's requirements and develop a unified inter-institutional methodology and related taxonomies for managing an inventory of software assets and an inventory of standards, targeting automated collection of data, preferably based on existing customer's processes.

Task 2: Propose tools to perform periodic inter-institutional inventories of software assets and standards

The contractor will prepare a list, together with necessary justifications, of tools which can be used for keeping and consolidating an inventory of software assets and standards, targeting regular automatic collection of data from systems existing in the European Commission and the European Parliament. The list will also contain information crucial for subsequent selection of tools by the European Commission and the European Parliament.
Task 3: Support in the selection and acquisition of tools, their installation and configuration

The contractor will assist the European Commission and the European Parliament in the choice of the final set of tools to use for the execution of Work Package 4 (inventory of software assets) and Work Package 5 (inventory of standards). The contractor will assist in the acquisition, installation and configuration of these tools in the European institutions' premises, including integration with the existing tools.

Work Package 4


The contractor will prepare full inventory of Open Source Software used in the European Commission and the European Parliament using tools selected and metrics defined in Tasks 1, 2 and 3.

Work Package 5

Task 5: Full inventory of open technical specifications used in the European Commission and the European Parliament

The contractor will prepare full inventory of open technical specifications used in the European Commission and the European Parliament using tools selected and metrics defined in Tasks 1, 2 and 3.

The work concerning all tasks mentioned above must involve close collaboration with the European Commission, the European Parliament and other project stakeholders and at least bi-weekly synchronisation meetings.

3. DETAILS ABOUT "DELIVERABLES" (different phases, tests, …)

As outcome of this study, the following deliverables will be provided:

– **Deliverable 1**: Methodology described in Task 1 in the form of a comprehensive written report.

– **Deliverable 2**: Proposition described in Task 2 in the form of a written report.

– **Deliverable 3**: On-site presence as deemed necessary during the selection and acquisition process of tools to use for the inventories' consolidation.

– **Deliverable 4**: Installation and configuration of tools together with necessary documentation, with optional presence on-site, as deemed necessary.

– **Deliverable 5**: Delivery of communication and dissemination materials concerning Tasks 1, 2 and 3 in the form of executive summary, presentation and a flyer.

– **Deliverable 6**: Inventory described in Task 4 completed in the form described in Tasks 1, 2 and 3, with all the data present in the tool selected for the inventory and installed in Deliverable 4.

– **Deliverable 7**: Dissemination materials regarding the Task 4 in the form of a single-page executive summary, a concise presentation and a single-page flyer with visually attractive representation of the results.
– **Deliverable 8**: Inventory described in Task 5 completed in the form described in Tasks 1, 2 and 3, with all the data present in the tool selected for the inventory and installed in Deliverable 4.

– **Deliverable 9**: Dissemination materials regarding the Task 5 in the form of a single-page executive summary, a concise presentation and a single-page flyer with visually attractive representation of the results.

All deliverables will be provided to DIGIT in soft (.DOCX or .ODT, .PPTX or .ODP and .PDF) and hard copy (final version) in the English language.

The final delivery date for Deliverable 1 is set to the contract signature date plus 6 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 2 is set to the contract signature date plus 8 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 3 is set to the contract signature date plus 10 weeks. Earlier completion of the work is welcome.

The final delivery date for the Deliverable 4 is set to the contract signature date plus 14 weeks. Earlier completion of the work is welcome.

The final delivery date for the Deliverable 5 is set to the contract signature date plus 15 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 6 is set to the contract signature date plus 28 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 7 is set to the contract signature date plus 30 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 8 is set to the contract signature date plus 28 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 9 is set to the contract signature date plus 30 weeks. Earlier completion of the work is welcome.

**4. KEY SUCCESS FACTORS**

1. Existing tools will be analysed and tested and methodology for creating the inventory will be proposed, discussed and validated.
2. The specific requirements that must accomplish the methodologies and tools to be used in the creation of the inventory of assets and standards will be proposed.
3. The methodology to obtain the software inventory takes into account libraries, versions and dependencies between components.
4. Methodology to obtain the software inventory will let European Commission and European Parliament categorise the components by several criteria: criticality, existing support, areas where the components are used. Each component will be accompanied with information necessary to assess its sustainability, according to the metrics defined in Work Package 1 of FOSSA. Some examples known at the time of writing of this Technical Annex: development process, automatic regression testing, vulnerability reporting process, size of team supporting the project, financing of the team.
5. The list of free and open source software used by European Commission and European Parliament will be elaborated.

6. Levels of criticality are defined and validated, and classification of software following that criticality is made.

7. Extended information about each OSS component is obtained (E.g. community that is behind, type of licence).

8. Analysis of the application of the results of the Work Package 1 of FOSSA is made and conclusions are drawn.

9. The list of free and open technical specifications and open standards used by European Institutions is elaborated.

**5. OTHER PRECISIONS**

The job will be executed extra-muros with occasional visits on-site.

Given the project's specificity, the contractor must have a proven experience of working with the European Institutions.

The project description, as approved by the European Parliament, together with the project's Business Case and Project Charter documents are the accompanying sources of this work package's precise scope definition.

In case of specific tools necessary for completing the job (surveys, collaboration spaces, forums etc.), they will be hosted by the contractor. Hosting of the inventory software depends on the results of Work Package 3 (Tasks 1, 2 and 3).

Given the analysis and drafting quality expected, all contractors working for Deliverables 1, 2, 5, 7 and 9 must prove their experience in drafting high-level policy documents and proficiency in English (native speaker or CEFR English level C2 or equivalent).
TECHNICAL ANNEX – FOSSA WP3-5

1. CONTEXT / INTRODUCTION

This work is requested in the context of the Pilot Project "Governance and quality of software code – Auditing of free and open source software" (reference 26 03 77 02).

Recent discoveries of vulnerabilities in critical information infrastructure have drawn the broader public's attention to the need to understand how governance and quality of the underlying software code relates to basic safety and public trust in applications that are used on a day-to-day basis. As both the general public and the EU institutions regularly use free and open-source software - from end-user device applications to server systems - the need for coordinated efforts to ensure and maintain the integrity and security of that software has been highlighted by the European Parliament itself. This pilot project will offer a systematic approach to achieving a goal to which the EU institutions themselves can contribute, namely ensuring that widely used critical software can be trusted.

The project has been split into several work packages. This Technical Annex concerns Work Packages 3, 4 and 5 – preparation of a unified inventory methodology together with the necessary tools and preparation of inventories of free and open source software and open technical specifications used by the European Commission and the European Parliament.

2. DESCRIPTION OF TASKS

The contractor will perform the following tasks:

Work Package 3

Task 1: Development of a methodology to perform periodic inter-institutional inventories of software assets and standards

The contractor will collect the European Commission's and European Parliament's requirements and develop a unified inter-institutional methodology and related taxonomies for managing an inventory of software assets and an inventory of standards, targeting automated collection of data, preferably based on existing customer's processes.

Task 2: Propose tools to perform periodic inter-institutional inventories of software assets and standards

The contractor will prepare a list, together with necessary justifications, of tools which can be used for keeping and consolidating an inventory of software assets and standards, targeting regular automatic collection of data from systems existing in the European Commission and the European Parliament. The list will also contain information crucial for subsequent selection of tools by the European Commission and the European Parliament.
Task 3: Support in the selection and acquisition of tools, their installation and configuration

The contractor will assist the European Commission and the European Parliament in the choice of the final set of tools to use for the execution of Work Package 4 (inventory of software assets) and Work Package 5 (inventory of standards). The contractor will assist in the acquisition, installation and configuration of these tools in the European institutions' premises, including integration with the existing tools.

Work Package 4


The contractor will prepare full inventory of Open Source Software used in the European Commission and the European Parliament using tools selected and metrics defined in Tasks 1, 2 and 3.

Work Package 5

Task 5: Full inventory of open technical specifications used in the European Commission and the European Parliament

The contractor will prepare full inventory of open technical specifications used in the European Commission and the European Parliament using tools selected and metrics defined in Tasks 1, 2 and 3.

The work concerning all tasks mentioned above must involve close collaboration with the European Commission, the European Parliament and other project stakeholders and at least bi-weekly synchronisation meetings.

3. DETAILS ABOUT "DELIVERABLES" (different phases, tests, …)

As outcome of this study, the following deliverables will be provided:

- **Deliverable 1**: Methodology described in Task 1 in the form of a comprehensive written report.

- **Deliverable 2**: Proposition described in Task 2 in the form of a written report.

- **Deliverable 3**: On-site presence as deemed necessary during the selection and acquisition process of tools to use for the inventories' consolidation.

- **Deliverable 4**: Installation and configuration of tools together with necessary documentation, with optional presence on-site, as deemed necessary.

- **Deliverable 5**: Delivery of communication and dissemination materials concerning Tasks 1, 2 and 3 in the form of executive summary, presentation and a flyer.

- **Deliverable 6**: Inventory described in Task 4 completed in the form described in Tasks 1, 2 and 3, with all the data present in the tool selected for the inventory and installed in Deliverable 4.

- **Deliverable 7**: Dissemination materials regarding the Task 4 in the form of a single-page executive summary, a concise presentation and a single-page flyer with visually attractive representation of the results.
- **Deliverable 8**: Inventory described in Task 5 completed in the form described in Tasks 1, 2 and 3, with all the data present in the tool selected for the inventory and installed in Deliverable 4.

- **Deliverable 9**: Dissemination materials regarding the Task 5 in the form of a single-page executive summary, a concise presentation and a single-page flyer with visually attractive representation of the results.

All deliverables will be provided to DIGIT in soft (.DOCX or .ODT, .PPTX or .ODP and .PDF) and hard copy (final version) in the English language.

The final delivery date for Deliverable 1 is set to the contract signature date plus 6 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 2 is set to the contract signature date plus 8 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 3 is set to the contract signature date plus 10 weeks. Earlier completion of the work is welcome.

The final delivery date for the Deliverable 4 is set to the contract signature date plus 14 weeks. Earlier completion of the work is welcome.

The final delivery date for the Deliverable 5 is set to the contract signature date plus 15 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 6 is set to the contract signature date plus 28 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 7 is set to the contract signature date plus 30 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 8 is set to the contract signature date plus 28 weeks. Earlier completion of the work is welcome.

The final delivery date for Deliverable 9 is set to the contract signature date plus 30 weeks. Earlier completion of the work is welcome.

**4. KEY SUCCESS FACTORS**

1. Existing tools will be analysed and tested and methodology for creating the inventory will be proposed, discussed and validated.
2. The specific requirements that must accomplish the methodologies and tools to be used in the creation of the inventory of assets and standards will be proposed.
3. The methodology to obtain the software inventory takes into account libraries, versions and dependencies between components.
4. Methodology to obtain the software inventory will let European Commission and European Parliament categorise the components by several criteria: criticality, existing support, areas where the components are used. Each component will be accompanied with information necessary to assess its sustainability, according to the metrics defined in Work Package 1 of FOSSA. Some examples known at the time of writing of this Technical Annex: development process, automatic regression testing, vulnerability reporting process, size of team supporting the project, financing of the team.
5. The list of free and open source software used by European Commission and European Parliament will be elaborated.
6. Levels of criticality are defined and validated, and classification of software following that criticality is made.
7. Extended information about each OSS component is obtained (E.g. community that is behind, type of licence).
8. Analysis of the application of the results of the Work Package 1 of FOSSA is made and conclusions are drawn.
9. The list of free and open technical specifications and open standards used by European Institutions is elaborated.

5. OTHER PRECISIONS

The job will be executed extra-muros with occasional visits on-site.

Given the project's specificity, the contractor must have a proven experience of working with the European Institutions.

The project description, as approved by the European Parliament, together with the project's Business Case and Project Charter documents are the accompanying sources of this work package's precise scope definition.

In case of specific tools necessary for completing the job (surveys, collaboration spaces, forums etc.), they will be hosted by the contractor. Hosting of the inventory software depends on the results of Work Package 3 (Tasks 1, 2 and 3).

Given the analysis and drafting quality expected, all contractors working for Deliverables 1, 2, 5, 7 and 9 must prove their experience in drafting high-level policy documents and proficiency in English (native speaker or CEFR English level C2 or equivalent).

The EC can request revisions, corrections or modifications to each of the deliverables during one month after the reception.
Free and Open Source Software Auditing (FOSSA) Pilot Project

DISSEMINATION MATERIALS

Work Package 4 - EXECUTIVE SUMMARY

Work Package 4 (WP4) of the FOSSA Pilot Project prepared a full inventory of Open Source Software (OSS) used in the European Commission and the European Parliament. The applied methodology and architecture have been developed in Deliverables (DLV) 1, 2 and 3 of WP3. To evaluate OSS assets, both metrics developed by WP4 and the sustainability ones earlier defined by WP1 are implemented.

The inventory of OSS is based on the input data provided by the various stakeholders interviewed during the initial phase of the FOSSA project. As the information made available by the European Parliament on their IT assets did not allow performing an inventory of the OSS assets, such inventory focused for the time being only on the assets managed by the European Commission.

The inventory scope covered the infrastructure managed by DIGIT, including Datacenter applications and Desktop applications. The inventory provided results in two main respects: OSS screening / counting and critical OSS assessment:

1. Open Source Software screening / counting results

The screening and counting of software items and of their instances to weigh the OSS on the respective totals provided the following data:

- **Number of software items**

  - 82.86%
  - 18%

  - 38.017
  - 82%

  - Total: 46243
  - Open source software
  - Other software

- **Number of instances**

  - 16.082.297
  - 84%

  - 3.097.716
  - 16%

  - Total: 19.120.013
  - Open source software
  - Other software

This means that a minority, although significant, of all inventoried software in use at the European Commission is Open Source.

A few other facts:

- the top 4 OSS applications by number of instances (Firefox, Info-ZIP, VLC and Calibre) account for 1/3 of all OSS applications;
- as a consequence, the top three OS libraries / utilities are related with three of the top OSS applications (Firefox, VLC and Calibre);
- Almost all OS Operating Systems items refer to RedHat Enterprise Linux.

2. Detailed analysis of Open Source Software

The OSS in use at the European Commission was assessed under the following aspects:
• A **business criticality** evaluation, based on an analysis of the presence and use of OSS in the institutions. It took into account parameters such as the number of instances, the exposure to end users, the relation with security. The ranking of OSS by a **Business Criticality Index (BCI)**, based on such parameters, identified a **shortlist of the most critical software in use**, encompassing 22 items:

![OSS criticality ranking - shortlist](image)

• An assessment of OSS **sustainability**, based on the 34 metrics developed within WP1 of FOSSA project. Such metrics were used to evaluate the support that each of the Open Source projects is supposed to get from the community throughout its lifecycle to ensure its long-term success. The elements needed for such evaluation were collected through sources such as project websites, wikis, bugtrackers and some reputed platforms of the open source world (e.g. openhub.net or github.com).

The **overall sustainability**, calculated as the average of the 34 metrics (100% indicating top sustainability under all metrics), showed that the critical shortlist includes software with a **wide range of sustainability**, from 20% to almost 80%.

![Average of All Categories that Indicates Overall Sustainability of Analysed Projects](image)

The analysis has shown some limits in the actual availability and usability of data related to some metrics, particularly concerning the area of Performance (e.g. time spent in code reviews).

• Furthermore, the analysis of the **interdependencies** among the software items has identified the top software items by number of dependencies in the critical software shortlist:
<table>
<thead>
<tr>
<th>Components</th>
<th>Number of dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glibc</td>
<td>10 dependencies</td>
</tr>
<tr>
<td>Bash</td>
<td>8 dependencies</td>
</tr>
<tr>
<td>zlib, coreutils, libselinux, openssl-libs, system</td>
<td>4 dependencies</td>
</tr>
<tr>
<td>shadow-utils, libselinux, openssl-libs, system</td>
<td>3 dependencies</td>
</tr>
<tr>
<td>chkconfig, audit-libs, nss-utility, krb5-libs, pcre, nspr, nss-softokn-</td>
<td>2 dependencies</td>
</tr>
<tr>
<td>frebi, libcom_err</td>
<td></td>
</tr>
</tbody>
</table>
Dependencies analysis

The inventory analysis also covered one area that may amplify significantly the risks occurring in one of the inventoried OSS components: the dependencies Analysis performed on the Critical OSS shortlist.

<table>
<thead>
<tr>
<th>Components</th>
<th>Number of dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glibc</td>
<td>10</td>
</tr>
<tr>
<td>Bash</td>
<td>8</td>
</tr>
<tr>
<td>zlib, coreutils</td>
<td>4</td>
</tr>
<tr>
<td>shadow-utils, libutils, openssl-lib, system</td>
<td>3</td>
</tr>
<tr>
<td>chkconfig, audit-libs, nss-util, krb5-libs, pcres, nscr, nss-softokn-frebl, libcom_err</td>
<td>2</td>
</tr>
</tbody>
</table>

This analysis showed a relative fragmentation of the dependencies, apart from Glibc and Bash, on which depend respectively 10 and 8 software items of the shortlist.

For ongoing updates on FOSSA project status please visit: https://joinup.ec.europa.eu/community/eu-fossa/home
OSS counting

Inventory Scope:

Infrastructure managed by DIGIT, including Datacenter applications and Desktop applications.

Number of software items

- Total: 2228
- Other software: 38017
- About 16% of the total software installed and inventoried is Open Source.

Business Criticality analysis

EU-FOSSA defined a Business Criticality Index, based on three parameters:

- Number of instances of the software;
- Relation with security;
- Exposure to end-user.

The inventoried OSS was assessed based on this index. A shortlist of the top 22 critical OSS items was defined, on which to perform the subsequent detailed analysis.

Sustainability analysis

The critical OSS shortlist was assessed on sustainability metrics grouped in 6 categories (Community Activity, Performance, Quality and Security, Demographics and Diversity, Governance, FOSS support). The overall software sustainability is calculated as an average of those categories.

Average of All Categories that Indicates Overall Sustainability of Analysed Projects

- Apache 1.10.0
- WAMP 1.10.0
- WAMP 1.10.0
- Workstations - AppV
- Workstations - LANDesk
- Datacenter

<table>
<thead>
<tr>
<th>Software</th>
<th>Category 1</th>
<th>Category 2</th>
<th>Category 3</th>
<th>Category 4</th>
<th>Category 5</th>
<th>Category 6</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>0.8%</td>
<td>0.5%</td>
<td>0.3%</td>
<td>0.2%</td>
<td>0.1%</td>
<td>0.0%</td>
<td>0.3%</td>
</tr>
<tr>
<td>netbeans</td>
<td>0.4%</td>
<td>0.3%</td>
<td>0.2%</td>
<td>0.1%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Linux</td>
<td>2.1%</td>
<td>1.5%</td>
<td>1.2%</td>
<td>0.9%</td>
<td>0.7%</td>
<td>0.5%</td>
<td>1.1%</td>
</tr>
<tr>
<td>NetBeans</td>
<td>0.5%</td>
<td>0.4%</td>
<td>0.3%</td>
<td>0.2%</td>
<td>0.1%</td>
<td>0.0%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Apache</td>
<td>0.8%</td>
<td>0.5%</td>
<td>0.3%</td>
<td>0.2%</td>
<td>0.1%</td>
<td>0.0%</td>
<td>0.3%</td>
</tr>
</tbody>
</table>
Inventory
Software
Open Source

Work Package 4

- FOSSA
and inventoried is Open Source (16%) or all software items installed.

A minority, although significant, total of 19.120.013 amounts up to 3.037.716 on a.
The number of instances of OSS (46.243).

Software Items (8.226) out of a significant part of the total amount and managed by DIGIT amount use at the European Commission.

Open Source Software Items in

the European Commission

SW counting & screening OSS at
ANALYSIS AND RANKING

OSS IST

Criticality ranked by OSS IST

Exposure to end user

Index (CI)
Critcality

Security
Relation with instances of number of

BUSINESS CRITICALITY ANALYSES
From 20% (very low) to almost 80% (high).

The sustainability of the critical software ranges

34 sustainability metrics (Community Activity, Performance, Quality, and Security).

The critical OSS shortlist was assessed on...
This analysis shows a relative fragmentation of the dependencies, apart from glibc:

<table>
<thead>
<tr>
<th>Component</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treli, Libgcc-err</td>
<td>2</td>
</tr>
<tr>
<td>chcon, libid, nss-ntl, krb5-libs, gconf, nspr, nss-sokia</td>
<td>3</td>
</tr>
<tr>
<td>shadow-utils, libssl, OpenSSL, gmp, system</td>
<td>4</td>
</tr>
<tr>
<td>zlib, curl-utils</td>
<td>8</td>
</tr>
<tr>
<td>bash</td>
<td>10</td>
</tr>
<tr>
<td>glibc</td>
<td>10</td>
</tr>
</tbody>
</table>

The following components have more than 1 dependency upon the shortest:

- glibc

The inventory also analyzed the dependencies within the critical OSS shortlist.

The dependency analysis