Free and Open Source Software Auditing (FOSSA) Pilot Project

DISSEMINATION MATERIALS

Work Package 2 - EXECUTIVE SUMMARY

The FOSSA Pilot Project aims at providing a systematic approach for the EU Institutions to contribute to Free and Open Source Software (FOSS). It will help reinforce the contribution of EU Institutions to ensure and maintain the integrity and security of key FOSS.

As part of the scope of the FOSSA Project, the objectives of WP2 are to develop a methodology for conducting code reviews and a feasibility study framework for open source projects, resulting in two deliverables:

1. A **Code Review Methodology** which approach relies on the selection of one (or several) code review tools, a team with clearly defined roles and responsibilities and a process for communicating the results of the code review.

   The Code Review Methodology covers four phases:

   - **Planning:** definition of scope, objectives, stakeholder engagement, constraints of the code review and testing environment;
   - **Execution:** both automated and manual tests are carried out, using the control checklists developed for Java, PHP, C and C++;
   - **Assessment:** analysis and evaluation of the findings, impact analysis and prioritisation;
   - **Reporting:** reporting of the results to the stakeholders.

   Stakeholders engagement was promoted through a methodology review and a validation workshop. Feedback from FOSS communities has also been requested through the JoinUp platform.

2. A **Feasibility Study Framework** that provides a mechanism to analyse the viability of a code review project, based on the project requirements and limitations.

   To reach the objective, the following tasks are conducted:

   - The project requirements are gathered and classified in five aspects:
     - **technical:** evaluates the knowledge and tools factors required to execute the project;
     - **economic:** evaluates the cost, cost limit and benefit factors;
     - **legal:** evaluates the tool license factor;
     - **operational:** evaluates the required project staff, the stakeholders, the code and its documentation, the applied methodology and the scope factors;
     - **scheduling:** evaluates the time and time limit factors.

     Each aspect and its relevant requirements are evaluated for the potential impact on the project.
   - The project limitations are defined: scope, time and cost. These limits provide the framework for the requirements of the feasibility study;
   - All the information gathered is analysed to determine whether the project is feasible or not. In case of a negative result, some of the requirements shall to be modified

All the deliverables are based on information gathering, consolidation and analysis. The team uses reputable sources of information for its research (among them OWASP, ITIL and GitHub).

Finally, the Code Review Methodology will be tested during WP6, and the Feasibility Study Framework can be used before engaging in new Open Source Software project. Correctly implemented and followed, the Code Review process could become an ongoing activity within the European Institutions.