# Free and Open Source Software Auditing (FOSSA) Pilot Project

## DISSEMINATION MATERIALS

## Work Package 1 - EXECUTIVE SUMMARY

The FOSSA Pilot Project aims at a systematic approach for the EU Institutions to contribute to Free and Open Source Software (FOSS). It will help reinforcing 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 main objective of WP1 is to elaborate a C**omparative Study** of the software development best practices used in respectively the EU Institutions and FOSS Communities.

To develop the C**omparative Study**, the FOSSA team conducted interviews with owners of 14 EU Institutions Projects and representatives from another 14 FOSS Communities. According to this process, existing software development best practices were collected, analysed and compared. This resulted in a set of recommendations for both EU Institutions Projects and FOSS Communities.

Besides the Comparative Study, WP1 delivers two other documents that provide the necessary tools to further increase the use of FOSS in the EU Institutions together with improving the quality of the software:

1. A set of **Metrics to Evaluate the Sustainability of a Free and Open Source Project.**

   If you are going to rely on a FOSS Community contribution-based project for your own project, you want to ensure its continuous support throughout the lifecycle of your project. For any Free and Open Source Project, the sustainability of its community is fundamental for its long term success. The project team defined 34 measurable Metrics (grouped in six categories) useful to measure and evaluate the Sustainability of FOSS Projects.

2. A **Governance Model:**

   The proposed Governance Model encompasses five governance areas together with their related processes and roles & responsibilities. The team conducted a series of electronic surveys to gather information on the existing governance practices of EU Institutions and FOSS Communities and compared them with those defined in the Governance Model. This results in a number of recommendations to evolve the maturity of the existing governance practices

On the one hand, EU Institutions Projects will benefit from this study as it provides recommendations to improve their governance area.

On the other hand, FOSS Communities can also take advantage of the results of the study by implementing the relevant recommendations (if applicable within their particular community).

All the deliverables are based on information gathering, consolidation and analysis of existing practices already in use in the EU Institutions and FOSS Communities.

The team used reputable sources of information for its research, among which: OWASP, OSS Watch, ISACA, NIST… to align the documentation with worldwide used Best Practices and Standards.

Due to the nature of the FOSS Communities, it was difficult to gather information on their software development practices directly from their representatives, and this was a risk identified and mitigated by obtaining information from trusted sites such as the FOSS Communities websites, recognised wikis and forums.

To conclude, FOSSA WP1 identified **Best Practices for FOSS Development and Governance**. When correctly implemented and followed, this leads to a more secure and organised software development lifecycle. On top of it, the produced set of Metrics enables evaluating the Sustainability of FOSS Projects.