European Commission

# WP1

# Index

*Analysed Projects and Communities*

*Main Deliverables and Objectives*

- **Comparative Study**
- **Metrics Definition for FOSS (Free and Open Source Software) Sustainability**
- **Governance Model**


# FOSS Communities analysed in the project


















# Comparative Study - Overview

*Study compares software security practices used in the software development life cycle (SDLC) phases*

*Less governed areas identified:*

- *Project Management (PM) conducted in an informal way by FOSS communities*
- *Software security in EU institutions with areas for improvement* in the SDLC

*Main findings and Recommendations:*

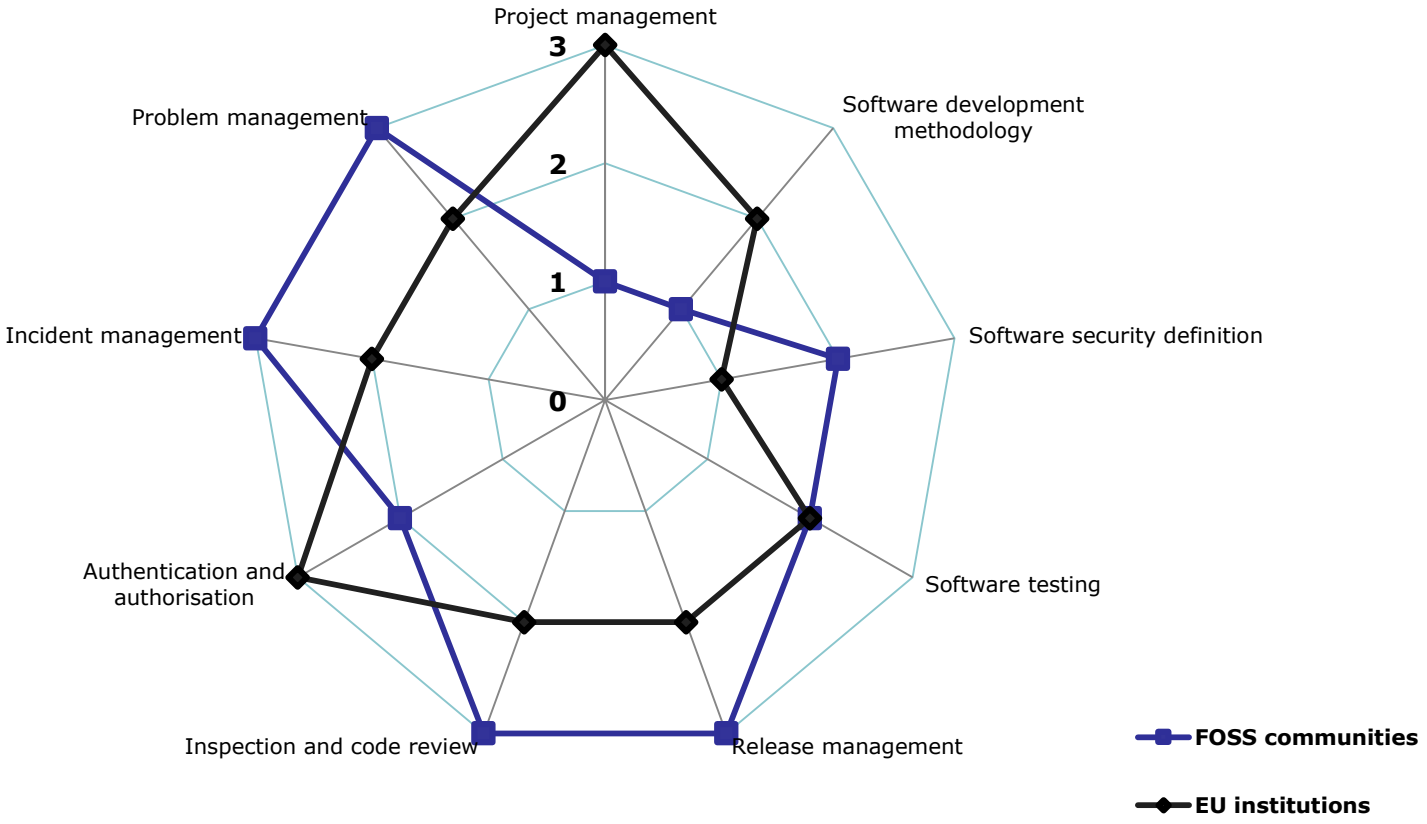
*FOSS communities*

- use formal methodologies for PM and software development
- promote PM contributions in the community

*European institutions*

- improve software security (definition, review, response) for all their projects

# Comparative Study Results




**1**: Minimum compliance. Improvement needed

**2:** Partially compliant. Can be improved

**3:** Compliant

# Metrics Definition for FOSS Sustainability

*34 metrics defined, divided in six categories:*

- Community Activity
- Performance
- Quality and Security
- Demographics and Diversity
- Governance
- FOSS support

*For each metric, associated criteria defined: description, unit of measurement, method of measurement, frequency, responsible for the measurement.*

*Each metric measured, resulting score shown in a graphic way.*

# Governance Model - Overview

*Identified 5 Governance Areas with corresponding processes*

*Governance Model proposed, based on international standards.*

*Governance practices compared / Recommendations provided:*

*FOSS communities*

- clearly define business-related roles and responsibilities
- ensure project support throughout its lifecycle (*)
- define and classify software requirements (*)
- Provide continuous financial support / offer value-added services

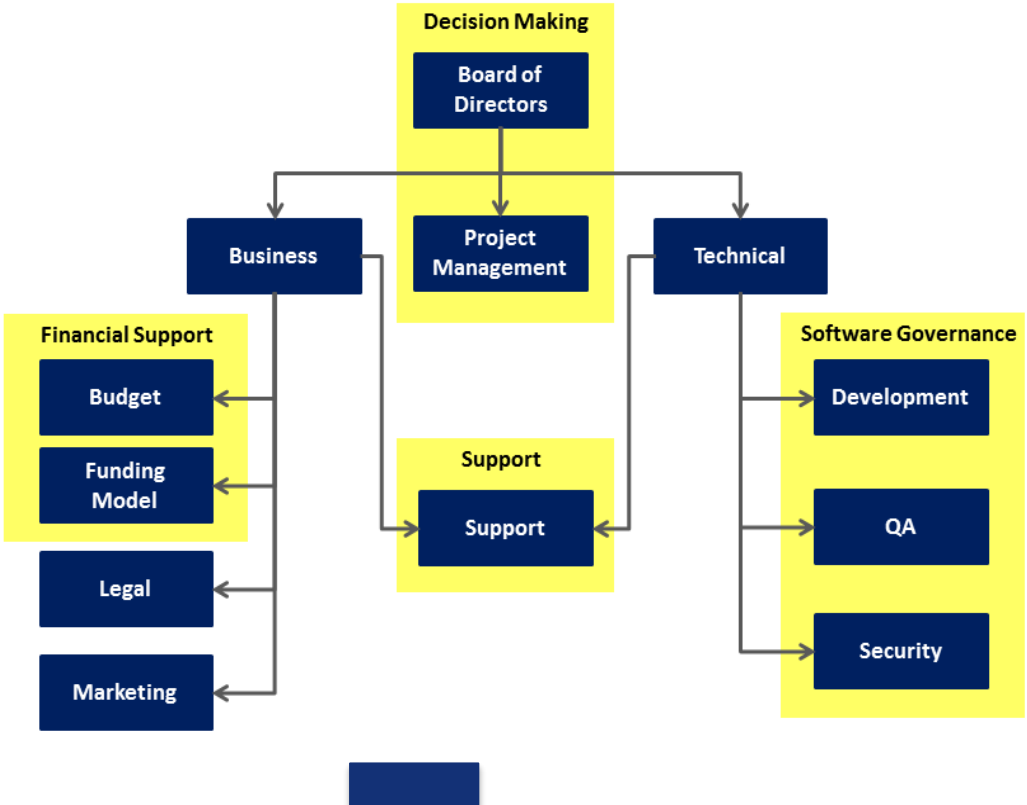
*European institutions*

- keep documentation up-to-date
- be aligned with business objectives
- define and classify software requirements

*(*) Applies to both EU Institutions and FOSS communities*

# Governance Model – Proposed organisation

*Organisation is based on identified Software Development areas and necessities. The areas highlighted in yellow correspond to the Governance Areas that are directly related to Software Security*



European Commission

# Thank you!