Feasibility of the Code Review

Provides a mechanism to analyse the viability of a code review project.

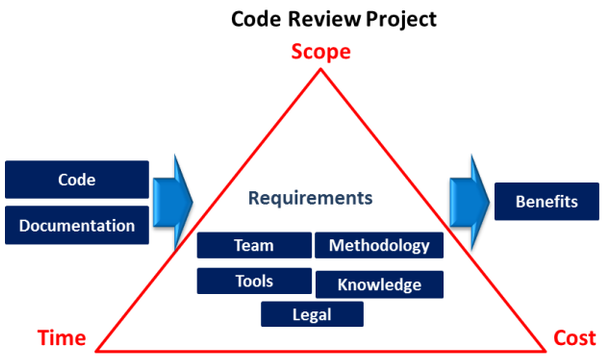
Project requirements:

- The team
- Knowledge
- Tools
- The project budget
- The benefits
- The legal issues that could arise
- The code
- The software documentation
- A methodology
- The project scope
- The time limit

These requirements are organised in 5 aspects as follows:

- ✓ Technical
- ✓ Economic
- ✓ Legal
- ✓ Operational
- ✓ Scheduling

All the information gathered is analysed to determine whether the code review project is feasible or not. If the result is negative, some of the requirements need to be modified



XX-00-00-000-EN-C

Do you want to collaborate?

Join us!

https://joinup.ec.europa.eu/community/eu-fossa/

Publications Office

ISBN 978-92-79-21088-4

doi:00.0000/00000

European Commission

FOSSA

Free and Open Source Software Auditing

Work Package 2:

Secure Code Review and Feasibility Study

DIGIT – B1

DIGIT

Planning the Code Review

Preparation

- ✓ Scope definition (software modules to analyse).
- ✓ Identifying needs (e.g. technical documentation of the code).
- ✓ Time and effort estimation.

Test Design

- ✓ Identifying the code review tool to use.
- ✓ Selecting the methodology mode (Managed, Defined or Optimised) per software module.
- ✓ Selecting the categories of the controls to apply for the code review.

Environment Configuration

- ✓ Installation and configuration of the code review tool (depending on the language).
- ✓ Installation of any other tools needed (e.g. IDE (Integrated Development Environment).

Executing the Code Review

Execution

- ✓ Managed Mode: Using automated tools to review common controls.
- ✓ Defined Mode: Manual mode to review common controls.
- ✓ Optimised Mode: Analysis of specific features of the software.

- Data/Input Management.
- Authentication Controls.
- Session Management.
- Authorisation Management.
- Cryptography.
- Error Handling/ Information Leakage.
- Logging/Auditing.
- Secure Code Design.

Managed and Defined Mode

- Concurrency.
- Denial-of-Service (DoS).
- Memory Management.
- Resource Management.
- Code structure
- Role/privilege matrix

Optimised Mode/ Specific Language controls

Results of the Code Review

Assessment

- ✓ Technical Report Analysis: It contains the results of the reviewed controls, as well as the documentation and classification of the findings.
- ✓ Impact Analysis: Analysing the findings to determine the Threat, Vulnerability and Impact, as well as the global risk per finding.
- ✓ Finding Prioritisation: Sorting the findings by the risk score to determine which of them should be fixed first.

Reporting

Different scope of reporting according to the code review objectives and results:

- ✓ **Internal** (European Institutions only)
- ✓ **Restricted** (European Institutions and external organisations, but not public)
- ✓ **Public**