



WP2



F  SSA

Free and Open Source Software Auditing

Index

1. List of requirements for code reviews

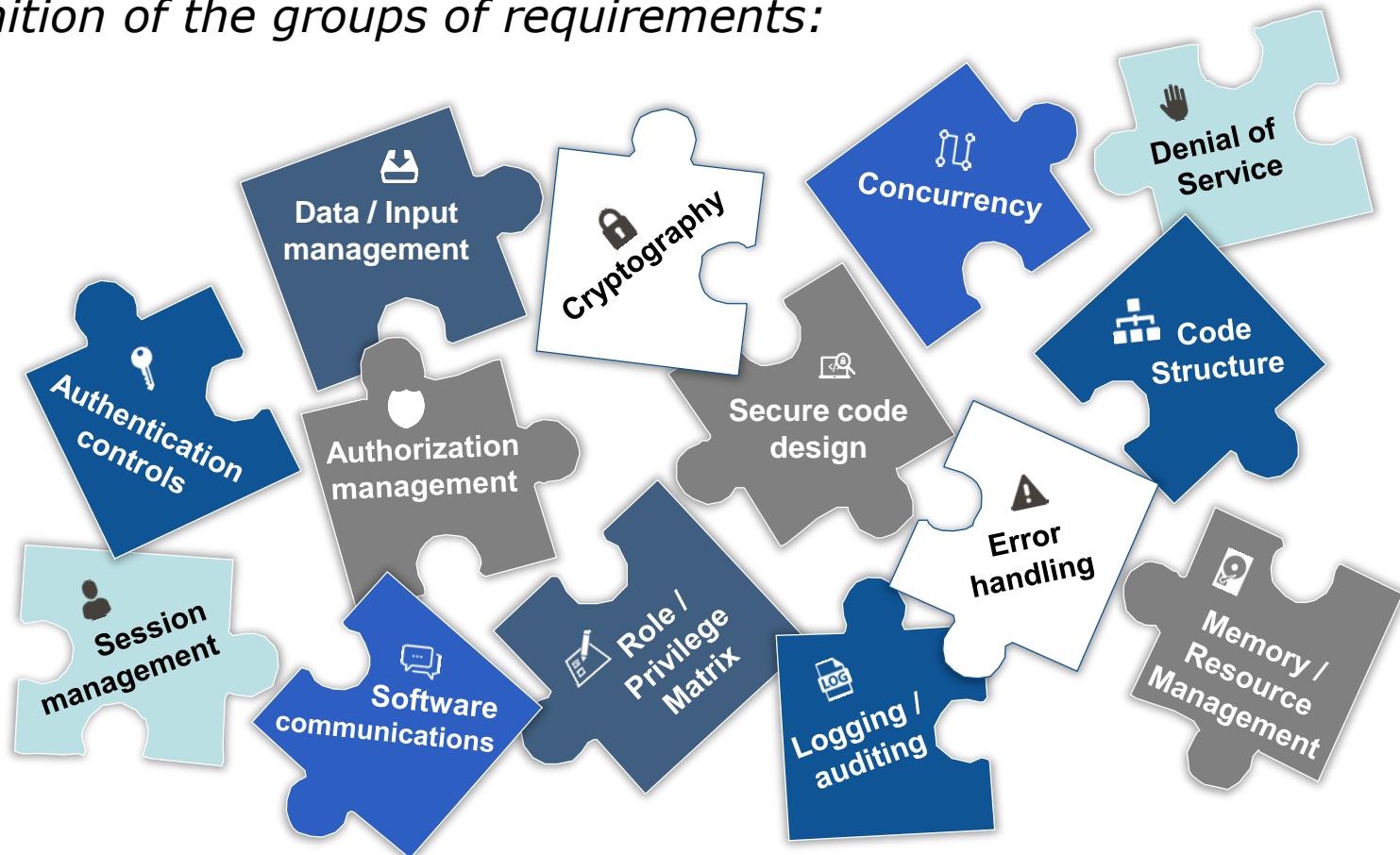
2. List of Tools and Methods for Communicating Results of Code Reviews

3. Design of the Method for Performing the Code Reviews for the European Institutions

4. Feasibility Study

List of requirements for code reviews

Definition of the groups of requirements:

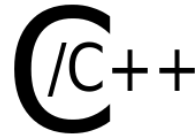


List of requirements for code reviews

Tools selected for code review depending on the language:



- FindBugs
<http://findbugs.sourceforge.net/>
- VCG
<https://github.com/nccgroup/VCG>
- Yasca
<http://www.scovetta.com/yasca.html>



- FlawFinder
<http://www.dwheeler.com/flawfinder/>
- RATS
<https://code.google.com/archive/p/rough-auditing-tool-for-security/>



- RIPS
<http://rips-scanner.sourceforge.net/>
- Yasca
<http://www.scovetta.com/yasca.html>

List of Tools and Methods for Communicating the Results of Code Reviews

Industry Standards

- **CVE** (Common Vulnerabilities and Exposures)
- **CWE** (Common Weakness Enumeration)
- **CVSS** (Common Vulnerability Scoring System)
- **CVRF** (Common Vulnerability Reporting Framework)



Proposed Tools



<https://www.atlassian.com/jira/>



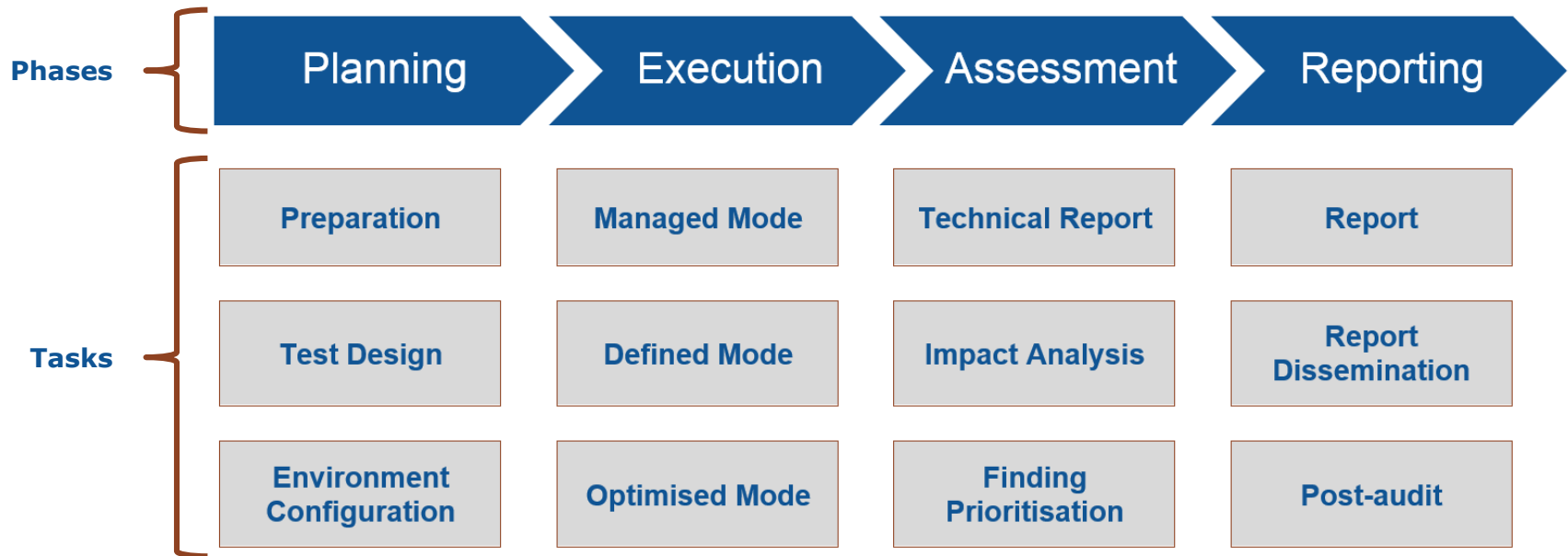
<https://joinup.ec.europa.eu/>



<http://jsreport.net/>

Design of the Method for Performing the Code Reviews for the European Institutions (1/4)

The methodology is divided into 4 phases:









Design of the Method for Performing the Code Reviews for the European Institutions (2/4)

The code review controls are grouped by their nature:

General controls

-  **Data/Input Management**
-  **Authentication Controls**
-  **Session Management**
-  **Authorization Management**
-  **Cryptography**
-  **Error Handling/Information Leakage**
-  **Software Communications**
-  **Logging/Auditing**
-  **Secure Code Design**

Optimised controls

-  **Concurrency**
-  **Denial of Service**
-  **Memory/Resource management**
-  **Code structure**
-  **Role/privilege matrix**
-  **Specific Language Controls**

Design of the Method for Performing the Code Reviews for the European Institutions (3/4)

Three different types of code review

Managed mode

- Automated review
- All controls included
- Initial vulnerabilities
- Additional weaknesses and bugs found

Defined mode

- Manual review
- Automated results validation
- Deep-level review of potential weak spots

Optimised mode

- Manual review
- In-depth analysis
- Language controls
- Review features that are context-dependant

Design of the Method for Performing the Code Reviews for the European Institutions (4/4)

Three distribution groups have been defined:

Internal



Only accessible to
European Institutions

Restricted



European Institutions and
external organisations, but
not the general public

Public

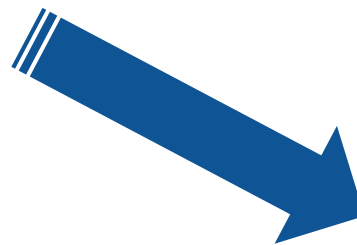
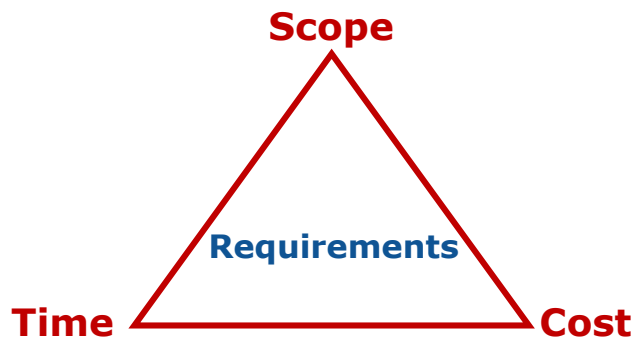


Anyone can see the
report

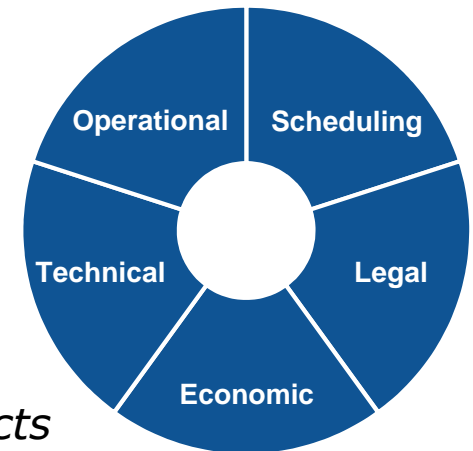
Feasibility study

The code review project needs to fulfil several requirements to be successful:

- Team
- Knowledge
- Tools
- Budget
- Potential legal issues
- Source code
- Software documentation
- Methodology
- Time restrictions



Requirements are organised into five aspects



*Finally, the information is analysed to determine the **project's feasibility**.*



Thank you!



Free and Open Source Software Auditing