# Comply Vanatage

# –

# Requirements and scope

## Project Features/Phases

### Phase 1: Feature - Develop Code Analyser (Java code only)

#### Business Problem

As a user want to be able to scan a java source code project so that I can identify which license types are used in the project so I can identify the risks

#### Description

* Implement Java code Validator
  + Should look at the input source code if it is valid Java. If not return a message to the user with a message indicating this
* Implement Java code analyser
  + Construct XML input file that is used for scanning criteria
  + Scan the java code to determine (copyright statements, license information) based on the above conditions
  + POM.xml should be fully scanned and analysed
  + Write the output of the scanning to XML file format

Nice to have – Should be discussed if we should pick this up as part of the project with SeQuenX:

* Output result saved and logged in Postgres

#### Acceptance criteria:

* Service should be developed as a microservice and run independently
* The service should integrateable with other developed micro services and/or scanning tools in the market ex: Fossology
* The service should be able to successfully scan a Java project
* The service should capture all used licenses and copy right statements
* The scanning results should be captured in XML formatted output file
* The performance should be acceptable and agreed with the stakeholders

### Phase 2: Feature – Java Dependency Checker

#### Business Problem

As a user want to be able to scan all maven dependencies of a java project so that I can identify which license types are used so I can identify the risks

#### Description

* Implement Java code Validator – See validator of the code analyser but usable for dependency checker
* Implement Java code dependency checker
  + Construct XML input file that is used for scanning criteria
  + Scan the java code to determine all used MVN dependencies based on the above
  + Write the output of the scanning to XML file format

#### Acceptance criteria:

* Service should be developed as a microservice and run independently
* The service should integrateable with other developed micro services and/or scanning tools in the market ex: Fossology
* The service should be able to successfully scan a Java project
* The service should capture all used MAVEN dependencies
* The scanning results should be captured in XML formatted output file
* The performance should be acceptable and agreed with the stakeholders

## Phase 3: Feature - Output generator – SPDX

#### Business Problem

As a user want to be able generate a BOM (Software Package Data Exchange (SPDX) file based on the scanning result of the code analyser and dependency checker micro service so I can identify the risks and import output in a workflow tool.

#### Description

* Store the scanning results in Postgres as preparation for generating the output
* Generate SPDX output format from stored scanning results in Postgres DB.
* Save the generate output with the scanning results in the DB

#### Acceptance criteria:

* Service should be developed as a microservice and run independently
* The service should integrateable with other developed micro services and/or scanning tools in the market ex: Fossology
* The service should be able to successfully scan a Java project
* The service should capture all used MAVEN dependencies
* The scanning results should be captured in XML formatted output file

## Phase 4: Integrate knowledge base to identify the risk

#### Business Problem

As a user want to be able generate a vulnerability report based on the generated BOM (SPDX) output so I can identify which vulnerabilities I need to resolve before releasing the product/source code.

#### Description

* Take the SPDX as input to generate the vulnerability report
* Create a Service that can consume the above input and integrates with the knowledge base
* Generate report in a XML format and store it with the scanning and BOM results in the database

#### Acceptance criteria:

* Service should be developed as a microservice and run independently
* The service should integrateable with any kind of Knowledge base service
* The service should be able to identify based on the BOM and Knowledge base the vulnerabilities and sort them based on the highest risk
* The report should be captured in XML formatted output file and stored with the scanning result and BOM output in the database