**Use Case 1**

* **Title**: Create New Policies or Update Policies
* **Primary Actor**: Manager
* **Goal in context:** Manager creates new policies or updates policies upon the policy retrieving from policy database.
* **Stakeholders**:
* Manager: To be able to retrieve policy for vulnerabilities and licenses from database and create or update the policy.
* **Preconditions**
* Manager sends the proper query.
* Relevant policies for vulnerabilities and licenses are in the database
* **Main Success Scenario:** Manager successfully creates new policies or edits policies.
* **Failed End Condition:** Manager cannot create new policies or edit policies, or manager create or update inaccurate policies.
* **Trigger:** Manager requests to create new policies or edit policies for licenses and vulnerabilities.

**Use case 2**

* **Title:** Determine the License and Vulnerability Information
* **Primary Actor:** Manager
* **Goal in context:** The manager of company is able to determine the licenses and vulnerabilities information from software package.
* **Stakeholders:**
* Manager: To receive clear and relevant software license and vulnerability information
* Developer: To provide the relevant file/software package information
* **Precondition:**
* Relevant file/license and vulnerability information is in the database.
* Proper software information has been provided.
* Proper query has been asked.
* **Main Success Scenario:** Manager receives accurate license and vulnerability information for the requested software packages.
* **Failed End Conditions:** Manager receives inaccurate or invalid license and vulnerability information for the requested software packages
* **Trigger**: Managers wants to determine the license and vulnerability information of software**.**

**Use Case 3**

* **Title:** Upload file for checking License and vulnerability
* **Primary Actor:** Developer
* **Goal in context:** To be able to upload software package and scan the package to get accurate vulnerability and license results.
* **Stakeholders:**
* Developer: To provide software package and receive the license and vulnerability results
* Manager: To oversee the process of checking the software package.
* **Precondition:**
* Developer upload the correct software package.
* OSS Management accept the software package.
* Fossology scan the software package and give the license results
* The software package name is checked in the NIST Vulnerability database and provide vulnerability results.
* **Main Success Scenario:** Developer uploads the software package successfully and receive the accurate results of licenses and vulnerabilities.
* **Failed End Conditions:** Developer cannot upload the software package or cannot get the accurate licenses and vulnerabilities results.
* **Trigger:** The software package need to be checked and developer uploads the proper software package.