

OPEN COMPLIANCE REFERENCE TOOLING

Open Compliance Reference Tooling

Welcome

- ▶ Marcel Kurzmann
- ▶ Working at Bosch.IO GmbH
- ▶ Represents Bosch in the OpenChain Governance board
- ▶ Regular participant of the tooling group
- ▶ INAL: I 'm not a lawyer!
- ▶ Disclaimer:
 - ▶ The following presentation is only for demonstration of the process and the tooling. The metadata was partly manipulated for the showcases.
 - ▶ If you plan to deploy a tool-suite comparable to the Open Compliance Reference Tooling please consult your legal team before applying license-classifications, rules and the output formats in your specific context.





Reference Tooling Work Group



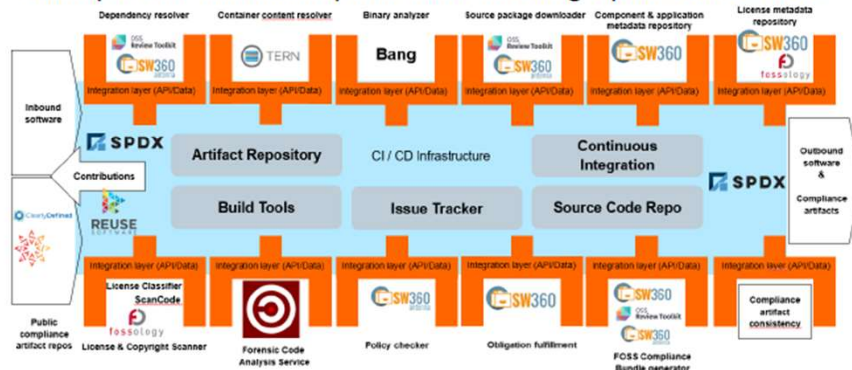
We are building an open source compliance toolchain ecosystem with open source tools as an open source project. To accomplish this we:

- Use existing independent tooling projects
- Provide reference workflows to allow their adoption
- Provide the concepts and glue to ensure easy interoperability and integration in existing environments
- Provide reference turnkey toolchains that can be used without fees by anybody

World-Wide Collaboration, World-Wide Availability



Example Automation Implementation Using Open Source Tools



Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: <https://groups.io/g/oss-based-compliance-tooling>

Online meetings: Bi-weekly - Invitations are sent to the mailing list

Website: <https://oss-compliance-tooling.org/>

And of course we are on GitHub:

<https://github.com/Open-Source-Compliance/Sharing-creates-value>

Open Compliance Reference Tooling

“Metadata debts”?



► “Technical debts” and “Metadata debts”

ISO/IEC DIS 5230:2020(E)
ISO #####-#:####(E)

3.3 Open source content review and approval

3.3.1 Bill of materials

A process shall exist for creating and managing a bill of materials that includes each open source component (and its identified licenses) from which the supplied software is comprised.

Verification material(s):

- ☐ 3.3.1.1 A documented procedure for identifying, tracking, reviewing, approving, and archiving information about the collection of open source components from which the supplied software is comprised.
- ☐ 3.3.1.2 Open source component records for the supplied software that demonstrates the documented procedure was properly followed.

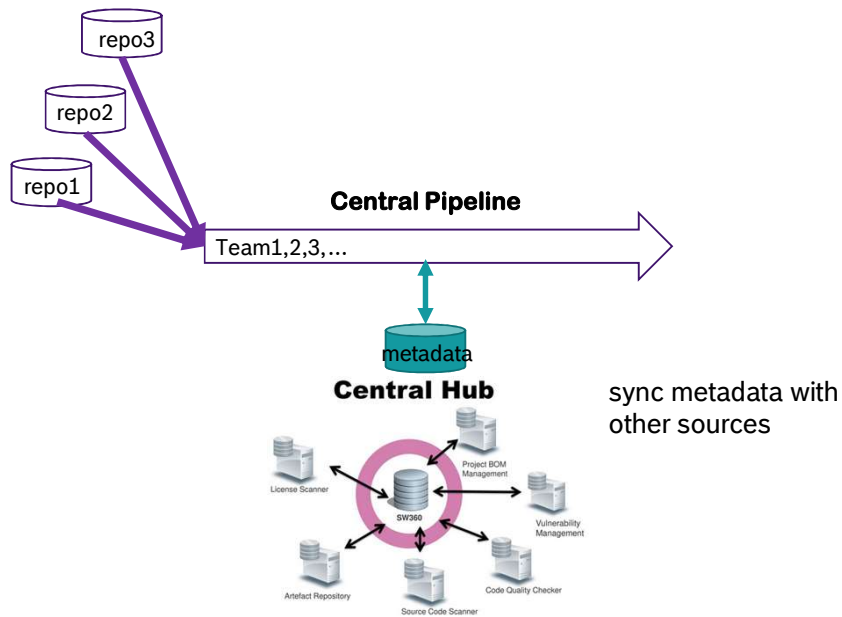
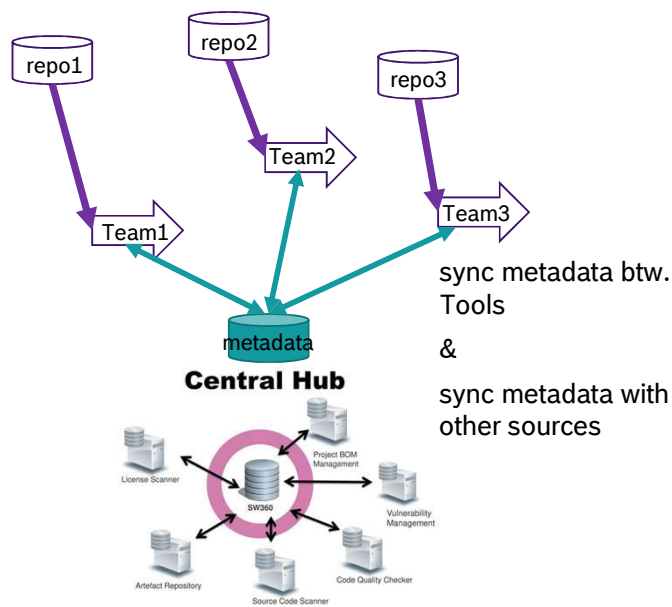
Rationale:

To ensure a process exists for creating and managing an open source component bill of materials used to construct the supplied software. A bill of materials is needed to support the systematic review and approval of each component's license terms to understand the obligations and restrictions as it applies to the distribution of the supplied software.

Open Compliance Reference Tooling

Range of application

- No single reference but depending on context e.g. heterogeneous vs. homogeneous OSM setups



Open Compliance Reference Tooling

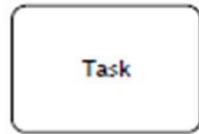
End to end process flow

- ▶ Business Process Modeling Notation
- ▶ Details see BPMN <http://www.bpmb.de/index.php/BPMNPoster>

- ▶ Events



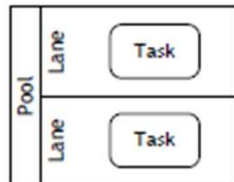
- ▶ Activities



- ▶ Gateways



- ▶ Lanes



Open Compliance Reference Tooling

And now ...

...the process in action

The process in bpmn and png + a role-description is available here:

<https://github.com/Open-Source-Compliance/Sharing-creates-value/tree/master/Tooling-Landscape/OpenComplianceReferenceTooling>

It is planned to enhance the process picture with a mapping to respective tools.

To keep it simple, the todays demo is based on OSS Review Toolkit as orchestrator.

In the scan step ScanCode will be used.

Open Compliance Reference Tooling

If you want to repeat steps on your own that I will present...

Preparation:

- ▶ Take a Windows Computer and create a new user (ideally with administrator rights)
- ▶ Install java from <https://www.codejava.net/java-se/download-and-install-java-11-openjdk-and-oracle-jdk> => OpenJDK11 ; set JAVA_HOME & set PATH as described
- ▶ Install python 3.6.8 from <https://www.python.org/ftp/python/3.6.8/python-3.6.8.exe>
- ▶ Install scancode toolkit 3.2.3 from <https://github.com/nexB/scancode-toolkit/releases> acc. to <https://scancode-toolkit.readthedocs.io/en/latest/getting-started/install.html> ; set PATH to scancode.bat
- ▶ Install git from <https://git-scm.com/download/win>
- ▶ Get a ort-binary (by building it on your own or from a colleague who has an IDE ready anyway)
- ▶ Install ort
- ▶ run “ort requirements”

Open Compliance Reference Tooling

Expected ort requirements feedback

```
status.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
OS = Windows_NT
COMSPEC = C:\WINDOWS\system32\cmd.exe
JAVA_HOME = c:\Program Files\Java\jdk-11.0.2

Scanners:
- Askalono: Requires 'askalono.exe' in version =0.4.3. Tool not found.
- BoyterLc: Requires 'lc.exe' in version =1.3.1. Tool not found.
- Licensee: Requires 'licensee.bat' in version =9.13.0. Tool not found.
+ ScanCode: Requires 'scancode.bat' in version =3.2.1-rc2. Found version 3.2.3.

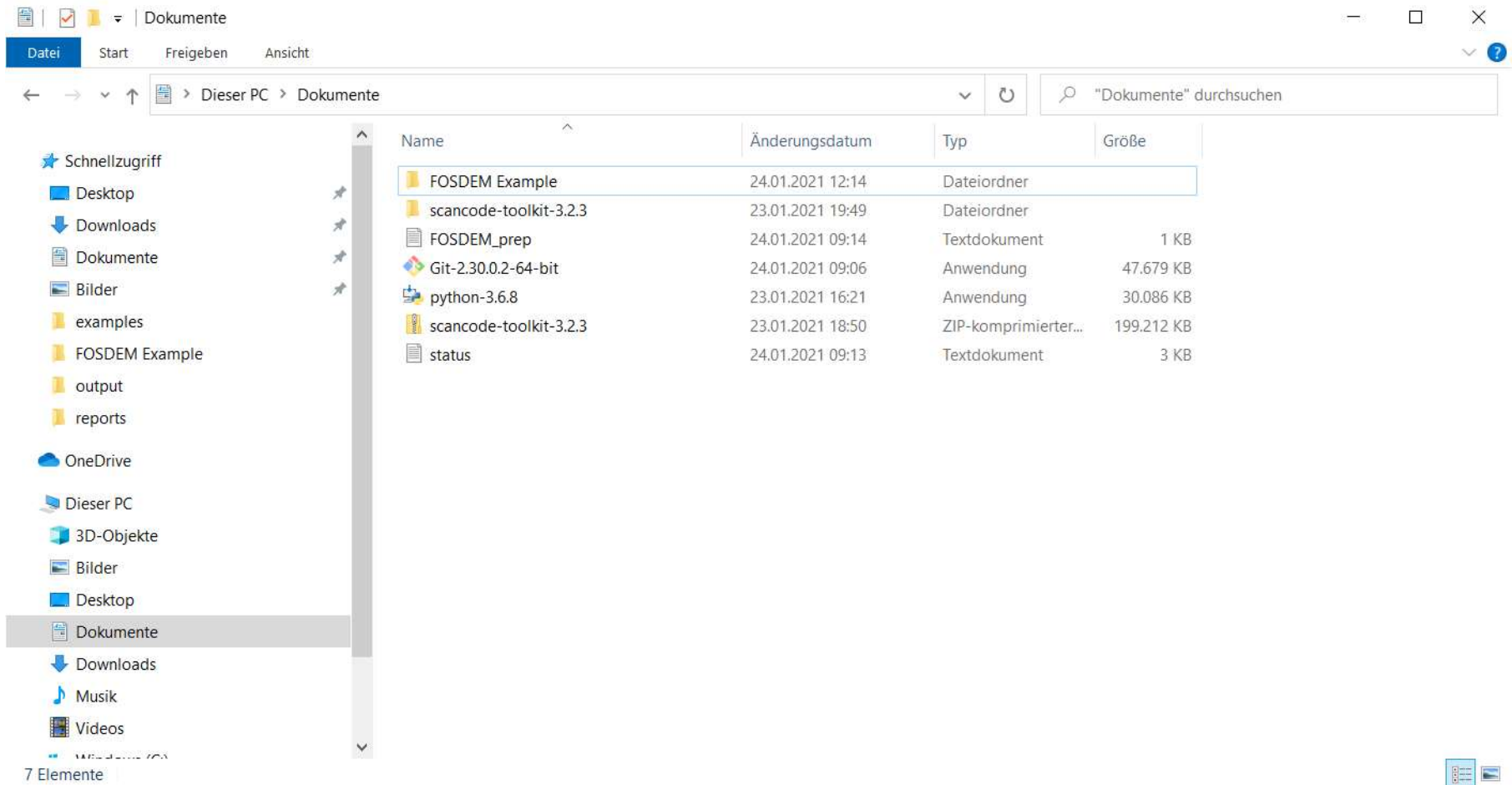
PackageManagers:
- Bower: Requires 'bower.cmd' in version >=1.8.8. Tool not found.
- Bundler: Requires 'bundle.bat' in version >=1.16.0. Tool not found.
- Cargo: Requires 'cargo' in no specific version. Tool not found.
- Composer: Requires 'composer.bat' in version >=1.5.0. Tool not found.
- Conan: Requires 'conan' in version >=1.18.0. Tool not found.
- GoDep: Requires 'dep' in no specific version. Tool not found.
- GoMod: Requires 'go' in no specific version. Tool not found.
- Npm: Requires 'npm.cmd' in version >=5.7.0 <6.15.0. Tool not found.
* Pip: Requires 'pip' in no specific version. Found version 18.1.
- Pipenv: Requires 'pipenv' in version >=2018.10.9. Tool not found.
- Pub: Requires 'pub.bat' in version >=2.2.0. Tool not found.
- Sbt: Requires 'sbt.bat' in version >=0.13.0. Tool not found.
- Stack: Requires 'stack' in version >=2.1.1. Tool not found.
- Yarn: Requires 'yarn.cmd' in version >=1.3.0 <1.23.0. Tool not found.

VersionControlSystems:
- Cvs: Requires 'cvs' in no specific version. Tool not found.
* Git: Requires 'git' in no specific version. Found version 2.30.0.windows.2.
- GitRepo: Requires 'repo' in no specific version. Tool not found.
- Mercurial: Requires 'hg' in no specific version. Tool not found.

Other tools:
* PythonVersion: Requires 'py' in no specific version. Found version 3.6.8.
- VirtualEnv: Requires 'virtualenv' in version >=15.1.0 <20.3.0. Tool not found.

Prefix legend:
- The tool was not found in the PATH environment.
+ The tool was found in the PATH environment, but not in the required version.
* The tool was found in the PATH environment in the required version.

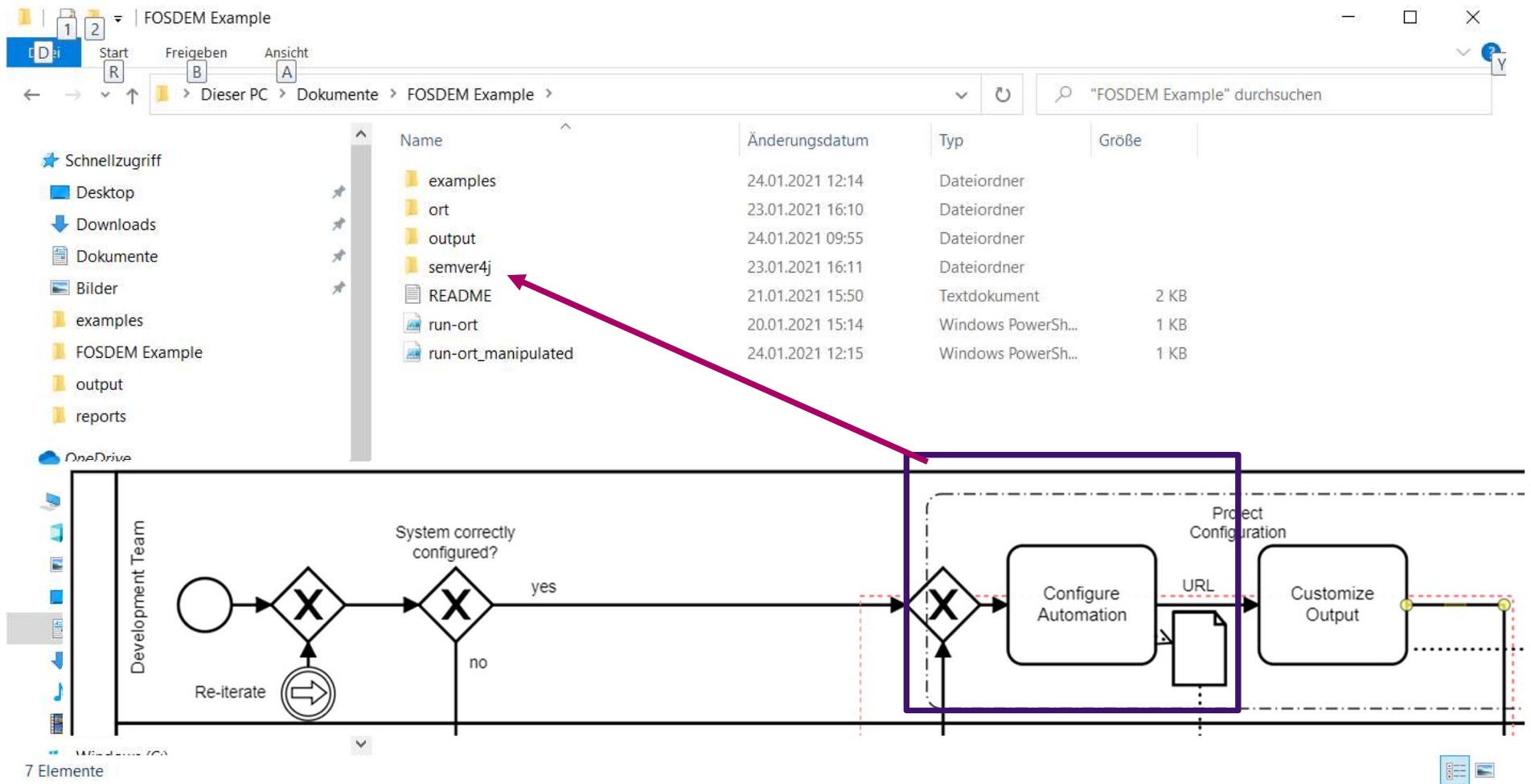
Not all tools were found in their required versions.
```



Open Compliance Reference Tooling

About the example...

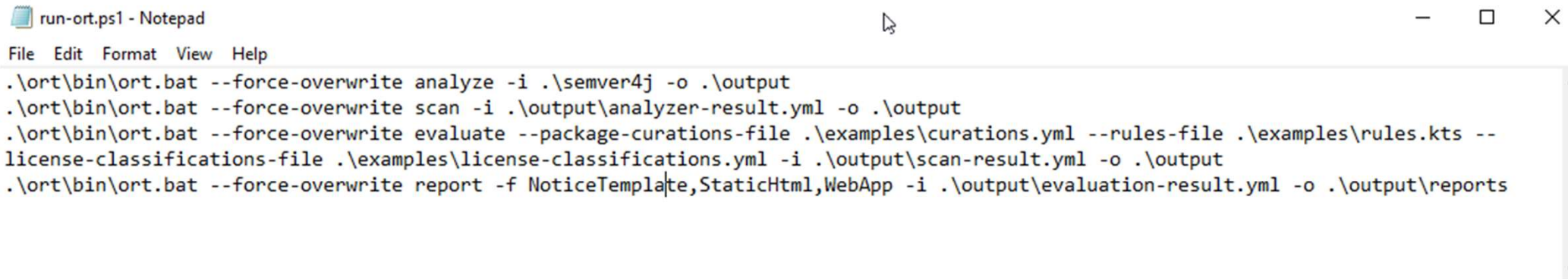
- ▶ Based on semver4j see <https://github.com/vdurmont/semver4j.git>
- ▶ Comes with a dependency to junit that will be used for the demo and some manipulations will be applied mainly to the ort-files



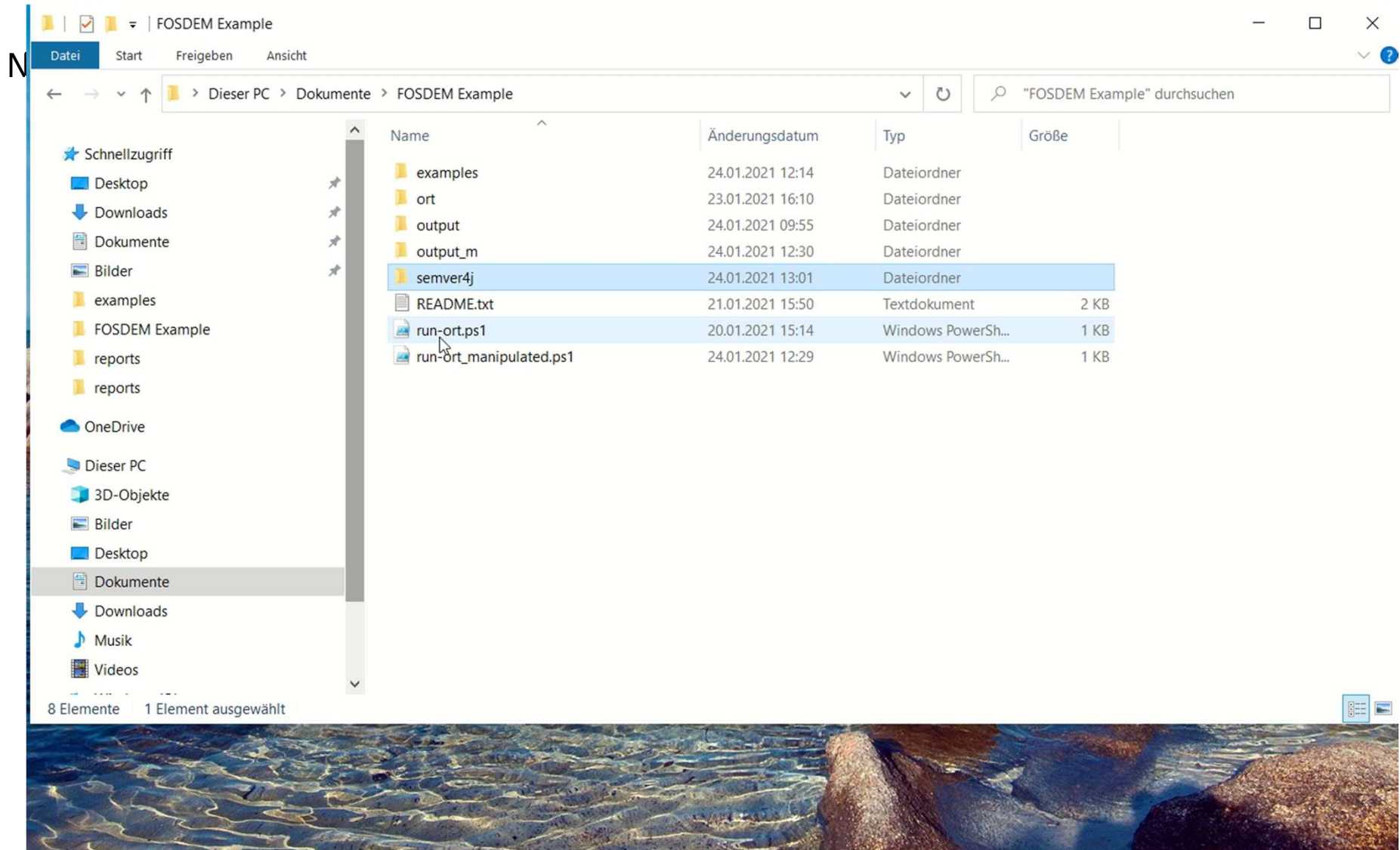
Open Compliance Reference Tooling

Happy Path

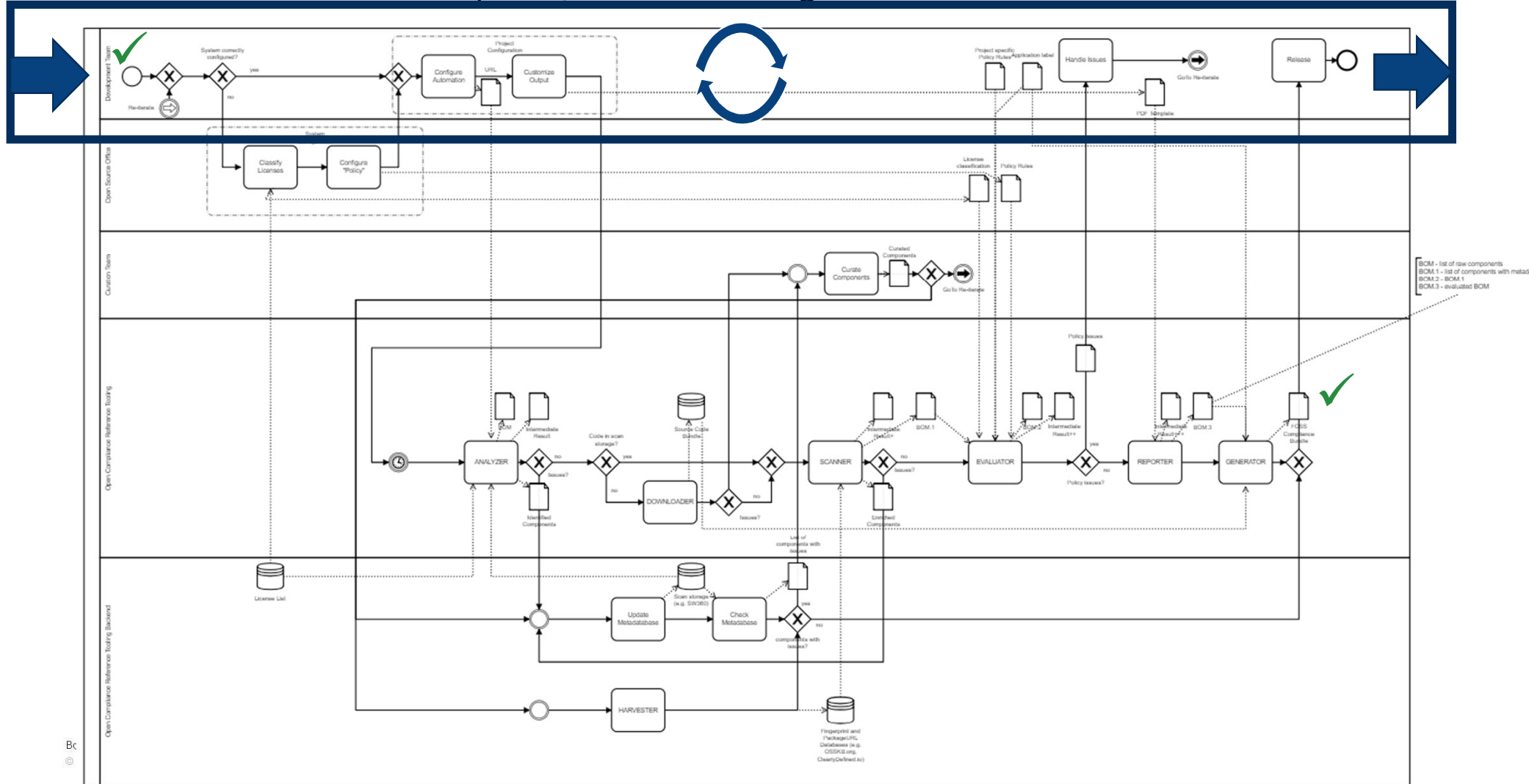
- Case 1: Continuous Development/Continuous integration => fast feedback



```
run-ort.ps1 - Notepad
File Edit Format View Help
.\ort\bin\ort.bat --force-overwrite analyze -i .\semver4j -o .\output
.\ort\bin\ort.bat --force-overwrite scan -i .\output\analyzer-result.yml -o .\output
.\ort\bin\ort.bat --force-overwrite evaluate --package-curations-file .\examples\curations.yml --rules-file .\examples\rules.kts --
license-classifications-file .\examples\license-classifications.yml -i .\output\scan-result.yml -o .\output
.\ort\bin\ort.bat --force-overwrite report -f NoticeTemplate,StaticHtml,WebApp -i .\output\evaluation-result.yml -o .\output\reports
```



Case 1: Continuous Development/Continuous integration => fast feedback



output

Start Freigeben Ansicht

Dieser PC > Dokumente > FOSDEM Example > output

"output" durchsuchen

Name	Änderungsdatum	Typ	Größe
downloads	24.01.2021 09:38	Dateiordner	
native-scan-results	23.01.2021 20:20	Dateiordner	
reports	24.01.2021 09:55	Dateiordner	
analyzer-result	24.01.2021 12:17	YML-Datei	6 KB
evaluation-result	24.01.2021 12:18	YML-Datei	221 KB
scan-result	24.01.2021 12:17	YML-Datei	220 KB

Schnellzugriff

- Desktop
- Downloads
- Dokumente
- Bilder
- examples
- FOSDEM Example
- output
- reports
- OneDrive
- Dieser PC
- 3D-Objekte
- Bilder
- Desktop
- Dokumente
- Downloads
- Musik
- Videos

6 Elemente

BOM - list of raw components
BOM.1 - list of components with metadata
BOM.2 - BOM.1
BOM.3 - evaluated BOM

reports

Datei Start Freigegeben Ansicht

< > > Dieser PC > Dokumente > FOSDEM Example > output > reports

"reports" durchsuchen

Name	Änderungsdatum	Typ
NOTICE_default	24.01.2021 12:18	
scan-report	24.01.2021 12:18	
scan-report-web-app	24.01.2021 12:18	

Schnellzugriff

- Desktop
- Downloads
- Dokumente
- Bilder
- examples
- FOSDEM Example
- output
- reports
- OneDrive
- Dieser PC
- 3D-Objekte
- Bilder
- Desktop
- Dokumente
- Downloads
- Musik
- Videos

3 Elemente

REPORTER

GENERATOR

Release

GoTo Re-iterate

PDF Template

PDF Report

FOSDEM Compliance

BOM - list of raw components
BOM.1 - list of components with metadata
BOM.2 - BOM.1
BOM.3 - evaluated BOM

Scan Report

Scan Report

Scan Report

+

←

→

🔄

🕒

Datei

|

C:/Users/Avatar/Documents/FOSDEM%20Example/output/reports/scan-report.html

🌟

🔖

🔗

👤

⋮

Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T12:04:21.038957100Z.

Project

Scanned revision 7653e418d610ffcd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index

[Rule Violation Summary \(0 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Rule Violation Summary (0 errors, 0 warnings, 0 hints to resolve)

No rule violations found.

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)

VCS Information

TypeGit

URLhttps://github.com/vdurmont/semver4j.git

Path

Revision7653e418d610ffcd2811bcb55fd72d00d420950b

Packages

#	Package	Scopes	Licenses	Analyzer Issues	Scanner Issues
1	Maven:com.vdurmont:semver4j:3.1.0		<div>Declared Licenses:</div> <div>MIT</div> <div>Detected Licenses:</div> <div>BSD-3-Clause (link to the location)</div> <div>MIT (exemplary link to the first of 3)</div>		

BOM - list of raw components
BOM.1 - list of components with metadata
BOM.2 - BOM.1
BOM.3 - evaluated BOM

Bosch.IO GmbH | 14.01.2021

© Bosch.IO GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution as well as in the event of applications for industrial property rights.

Open Compliance Reference Tooling

Reality – subset of potential real world cases

- ▶ Case 2:
 - ▶ Open Source Office issue: a license classification is missing
 - ▶ solution: Open Source Office provides an updated license-classifications.yml
- ▶ Case 3:
 - ▶ Development Team issue: a license is classified non-suitable to the context
 - ▶ solution: development team provides a new development increment where the component is removed
- ▶ Case 4
 - ▶ Development Team + Open Source Office issue: a license is classified non-suitable to the context
 - ▶ solution: development team excludes „test“ pattern in .ort.yml in project root directory
- ▶ Case 5
 - ▶ Curation Team issue: metadata missing for a dependency
 - ▶ solution: curation team investigates the situation and provides the metadata in curations.yml

Open Compliance Reference Tooling

Reality – subset of potential real world cases

▶ Case 2:

- ▶ Open Source Office issue: a license classification is missing
- ▶ solution: Open Source Office provides an updated license-classifications.yml

▶ Case 3:

- ▶ Development Team issue: a license is classified non-suitable to the context
- ▶ solution: development team provides a new development increment where the component is removed

▶ Case 4

- ▶ Development Team + Open Source Office issue: a license is classified non-suitable to the context
- ▶ solution: development team excludes „test“ pattern in .ort.yml in project root directory

▶ Case 5

- ▶ Curation Team issue: metadata missing for a dependency
- ▶ solution: curation team investigates the situation and provides the metadata in curations.yml

Case 2: Open Source Office - issue

Scan Report

← → ↺

📄 | 📄 | 📄

C:/Users/Avatar/Documents/FOSDEM%20Example/output_m/reports/scan-report.html

🌟 📌 🔗 👤 ⋮

Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T11:47:11.634923400Z.

Project
Scanned revision 7653e418d610ffd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j>.git

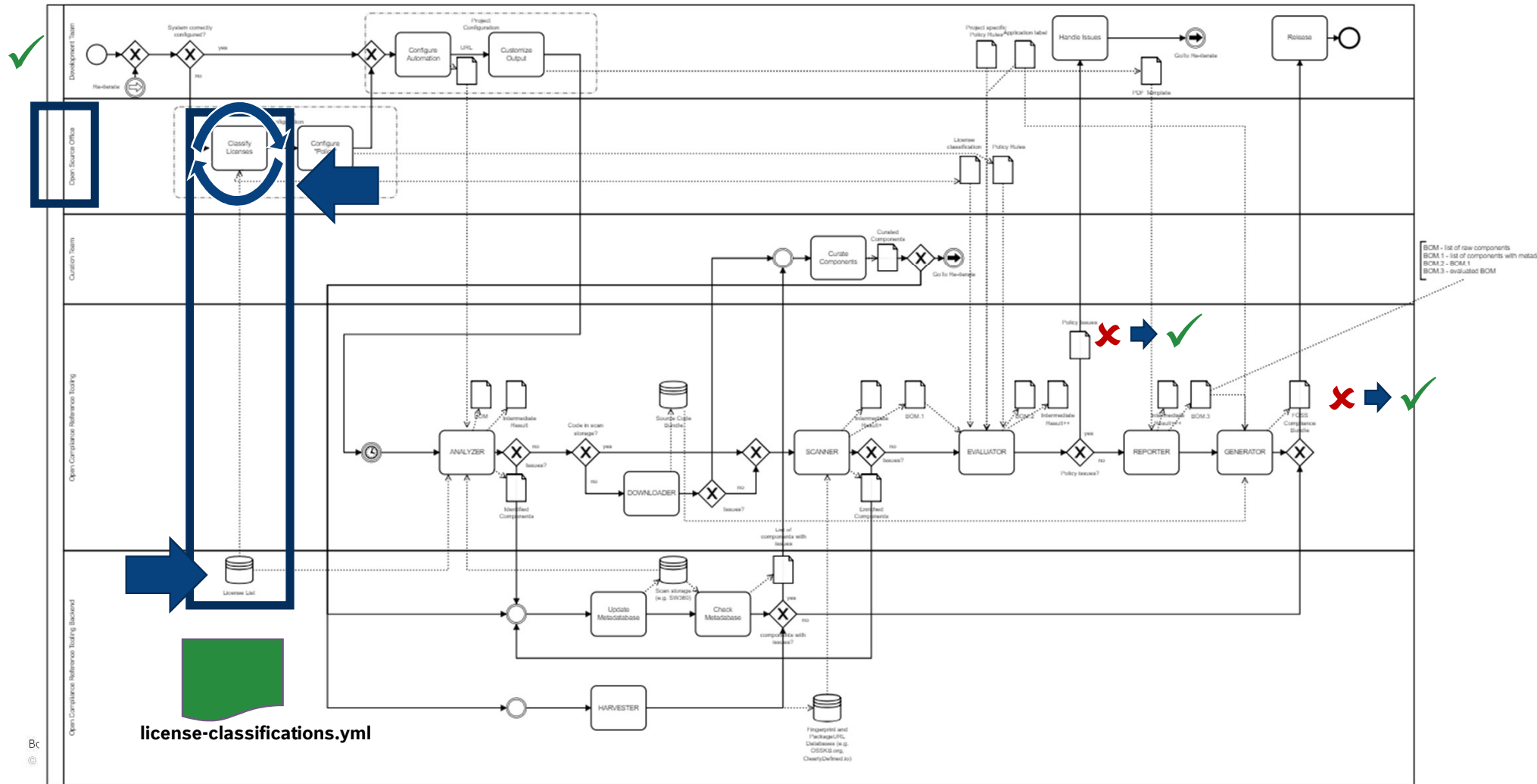
Index
[Rule Violation Summary \(3 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Rule Violation Summary (3 errors, 0 warnings, 0 hints to resolve)

#	Rule	Package	License	Message
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DECLARED: EPL-1.0	<p>The package Maven:junit:junit:4.12 has the declared ScanCode copyleft-limited categorized license EPL-1.0.</p> <p>► How to fix</p>
2	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: EPL-2.0	<p>The license EPL-2.0 is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12</p> <p>► How to fix</p>
3	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: NOASSERTION	<p>The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12</p> <p>► How to fix</p>

Bo: © BUSCH & GUTMANN 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution as well as in the event of applications for industrial property rights.

Case 2: Open Source Office - issue



Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T11:47:11.634923400Z.

Project

Scanned revision 7653e418d610ffcd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index

[Rule Violation Summary \(3 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Rule Violation Summary (3 errors, 0 warnings, 0 hints to resolve)

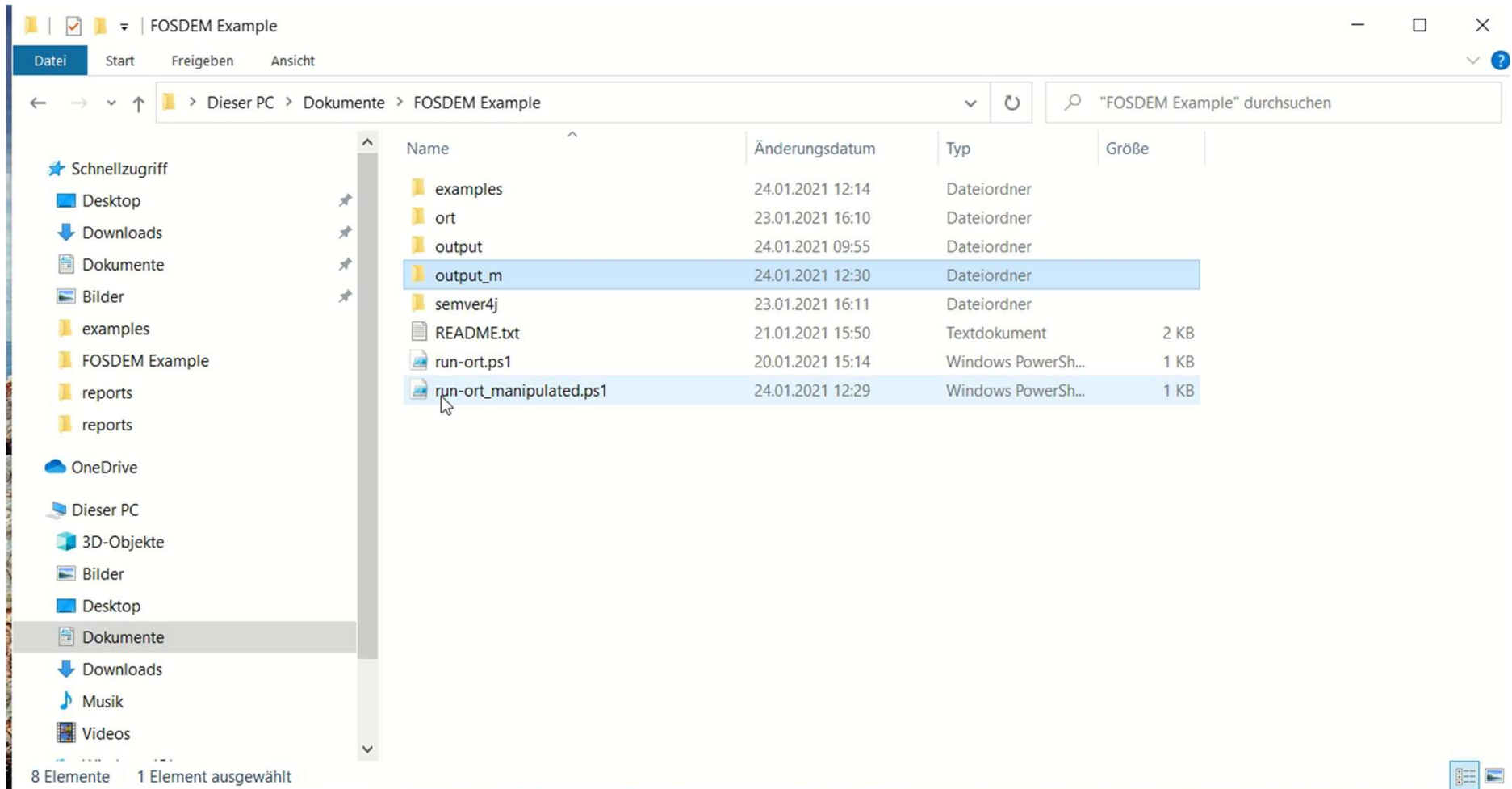
#	Rule	Package	License
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DECLARED: EPL-1.0
2	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: EPL-2.0
3	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: NOASSERTION

license EPL-1.0.
▶ How to fix

The license EPL-2.0 is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12
▶ How to fix

The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12
▶ How to fix

PROBLEM: License not classified
=> Open Source Office needs to
classify and
license_classification.yml needs to
be updated



Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T11:55:20.281914800Z.

Project

Scanned revision 7653e418d610ffcd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index

[Rule Violation Summary \(2 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Only 2 errors left!

Rule Violation Summary (2 errors, 0 warnings, 0 hints to resolve)

#	Rule	Package	License	Message
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DECLARED: EPL-1.0	The package Maven:junit:junit:4.12 has the declared ScanCode copyleft-limited categorized license EPL-1.0. How to fix
2	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: NOASSERTION	The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12 How to fix

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)

VCS Information

Type Git
URI <https://github.com/vdurmont/semver4j.git>

Open Compliance Reference Tooling

Reality – subset of potential real world cases

► Case 2:

- Open Source Office issue: a license classification is missing
- solution: Open Source Office provides an updated license-classifications.yml

► Case 3:

- Development Team issue: a license is classified non-suitable to the context
- solution: development team provides a new development increment where the component is removed

► Case 4

- Development Team + Open Source Office issue: a license is classified non-suitable to the context
- solution: development team excludes „test“ pattern in .ort.yml in project root directory

► Case 5

- Curation Team issue: metadata missing for a dependency
- solution: curation team investigates the situation and provides the metadata in curations.yml

Case 3: Development Team + Open Source Office - issue

Scan Report

Scan Report

← → ↺ ⓘ Datei | C:/Users/Avatar/Documents/FOSDEM%20Example/output/reports/scan-report.html

Scan Report

Created by **ORT**, the [QSS Review Toolkit](#), version f5a1d22 on 2021-01-24T11:55:20.281914800Z.

Project
Scanned revision 7653e418d610ffcd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index
[Rule Violation Summary \(2 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

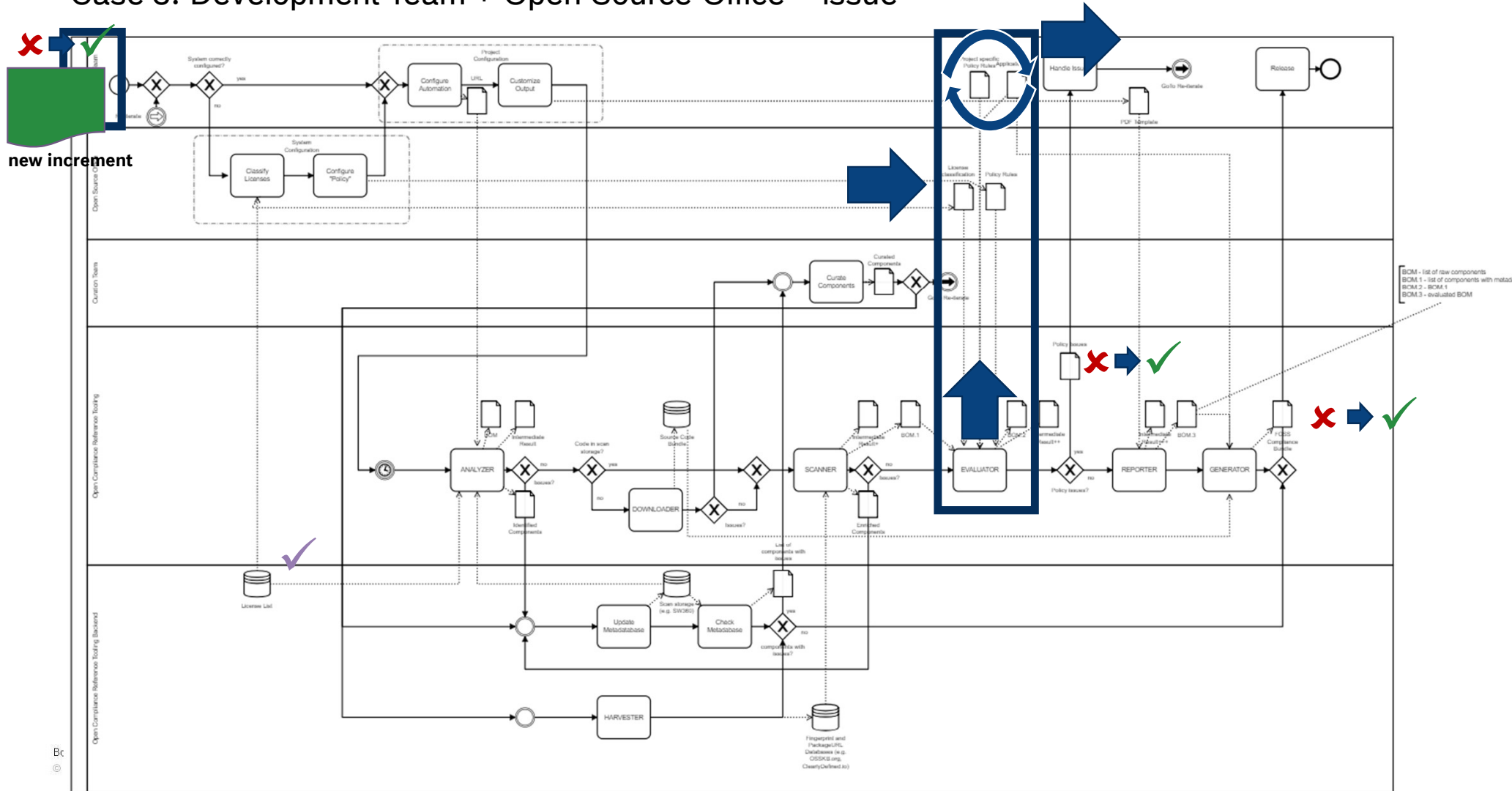
Rule Violation Summary (2 errors, 0 warnings, 0 hints to resolve)

#	Rule	Package	License	Message
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DECLARED: EPL-1.0	The package Maven:junit:junit:4.12 has the declared ScanCode copleft-limited categorized license EPL-1.0. ▶ How to fix
2	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: NOASSERTION	The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12 ▶ How to fix

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)
VCS Information
Type: Git
URI: <https://github.com/vdurmont/semver4j.git>

ISSUE for the Development Team:
License classification ok
=> Development Team needs to check
with Open Source Office if License
may be applied

Case 3: Development Team + Open Source Office - issue



Open Compliance Reference Tooling

Reality – subset of potential real world cases

► Case 2:

- Open Source Office issue: a license classification is missing
- solution: Open Source Office provides an updated license-classifications.yml

► Case 3:

- Development Team issue: a license is classified non-suitable to the context
- solution: development team provides a new development increment where the component is removed

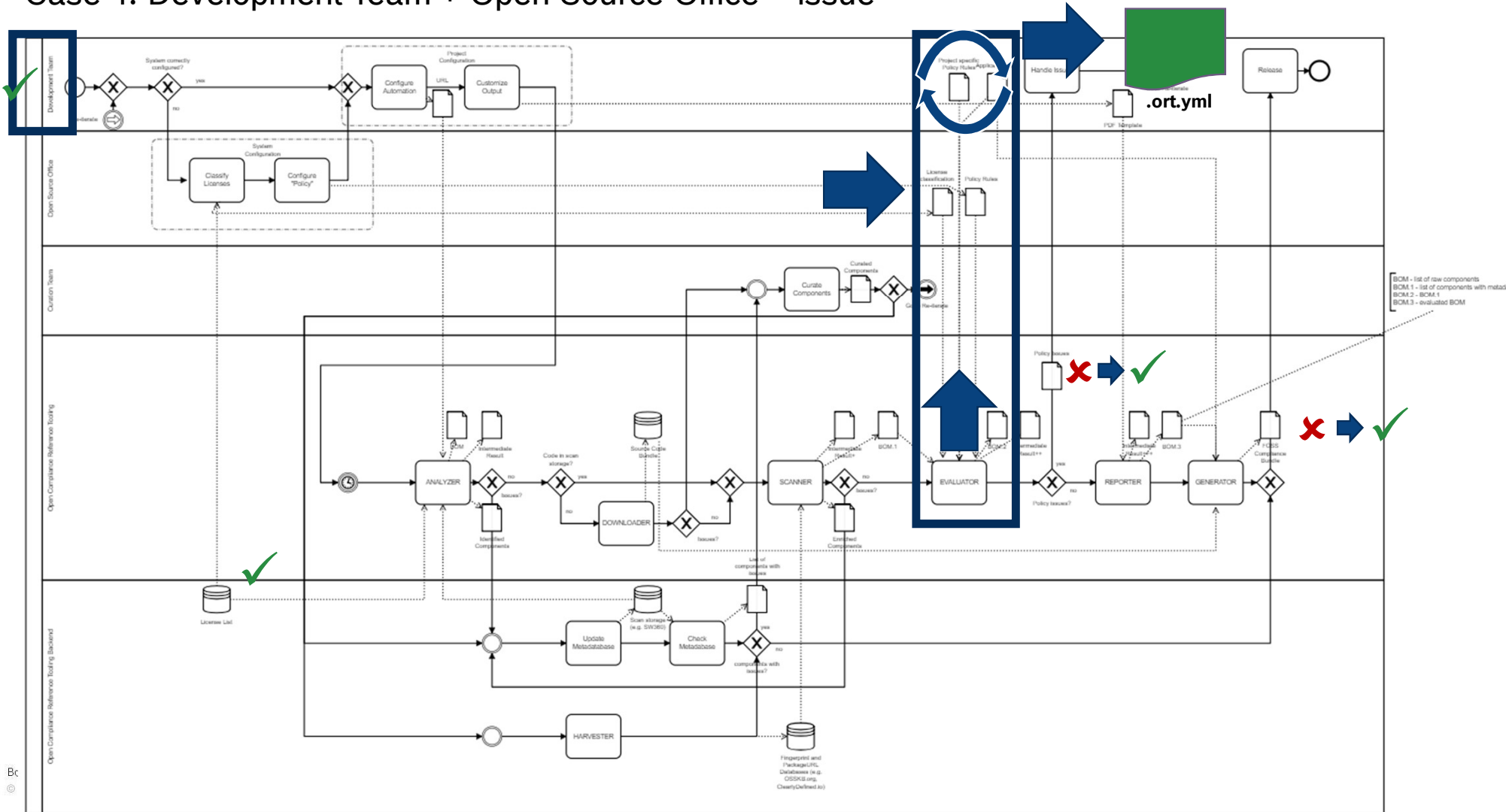
► Case 4

- Development Team + Open Source Office issue: a license is classified non-suitable to the context
- solution: development team excludes „test“ pattern in .ort.yml in project root directory

► Case 5

- Curation Team issue: metadata missing for a dependency
- solution: curation team investigates the situation and provides the metadata in curations.yml

Case 4: Development Team + Open Source Office - issue



Case 4: Development Team - issue

BUT – Development Team states that it is only for testing and will not be distributed! – team configures this in .ort.yml in the project repository root folder by excluding the „test“ pattern

The screenshot shows a Windows File Explorer window titled "semver4j" with the address bar path "Dieser PC > Dokumente > FOSDEM Example > semver4j". The left sidebar shows the "Dokumente" folder selected. The main pane displays a list of files and folders:

Name	Änderungsdatum	Typ	Größe
.git	23.01.2021 16:11	Dateiordner	
.github	23.01.2021 16:11	Dateiordner	
.idea	23.01.2021 16:11	Dateiordner	
ort	23.01.2021 16:11	Dateiordner	
src	23.01.2021 16:11	Dateiordner	
.gitignore	13.10.2020 11:43	Textdokument	1 KB
.ort.yml			
.travis.yml			
CHANGELOG.md			
LICENSE.md			
pom.xml			
prepared.ort.yml			
README.md			

The ".ort.yml" file is selected, and its contents are displayed in the ".ort.yml - Editor" window:

```
excludes:
  scopes:
    - pattern: "test"
      reason: "TEST_DEPENDENCY_OF"
      comment: "Packages for testing only."
```

The editor window shows the file is at "Ze 1, Sp 1" (Line 1, Column 1) with a zoom level of "100%", encoding of "Windows (CRLF)", and character set of "UTF-8".

Scan Report

Scan Report

Scan Report

+

←

→

↺

🕒

Datei

|

C:/Users/Avatar/Documents/FOSDEM%20Example/output/reports/scan-report.html

🔖

🔖

🔍

👤

⋮

Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T12:04:21.038957100Z.

Project

Scanned revision 7653e418d610ffcd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index

[Rule Violation Summary \(0 errors, 0 warnings, 0 hints to resolve\)](#)

[Maven:com.vdurmont:semver4j:3.1.0](#)

[Repository Configuration](#)

Rule Violation Summary (0 errors, 0 warnings, 0 hints to resolve)

No rule violations found.

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)

VCS Information

Type

Git

URL

<https://github.com/vdurmont/semver4j.git>

Path

Revision

7653e418d610ffcd2811bcb55fd72d00d420950b

Packages

#	Package	Scopes	Licenses	Analyzer Issues	Scanner Issues
1	Maven:com.vdurmont:semver4j:3.1.0		<div>Declared Licenses:</div> <div>MIT</div> <div>Detected Licenses:</div> <div>BSD-3-Clause (link to the location)</div> <div>MIT (exemplary link to the first of 3)</div>		

Bosch.IO GmbH | 14.01.2021

© Bosch.IO GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution as well as in the event of applications for industrial property rights.

Open Compliance Reference Tooling

Reality – subset of potential real world cases

- ▶ Case 2:
 - ▶ Open Source Office issue: a license classification is missing
 - ▶ solution: Open Source Office provides an updated license-classifications.yml
- ▶ Case 3:
 - ▶ Development Team issue: a license is classified non-suitable to the context
 - ▶ solution: development team provides a new development increment where the component is removed
- ▶ Case 4
 - ▶ Development Team + Open Source Office issue: a license is classified non-suitable to the context
 - ▶ solution: development team excludes „test“ pattern in .ort.yml in project root directory
- ▶ Case 5
 - ▶ Curation Team issue: metadata missing for a dependency
 - ▶ solution: curation team investigates the situation and provides the metadata in curations.yml

Case 5: Curation Team - issue

Packages					
#	Package	Scopes	Licenses	Analyzer Issues	Scanner Issues
1	Maven:com.vdurmont:semver4j:3.1.0		<p>Declared Licenses:</p> <p>MIT</p> <p>Detected Licenses:</p> <p>BSD-3-Clause (link to the location) MIT (exemplary link to the first of 3 locations)</p>	<p>ISSUE for the Curation Team: Component detected with „No Assertion“ => Curation Team needs to investigate the situation</p>	
2	Maven:junit:junit:4.12	test	<p>Declared Licenses:</p> <p>EPL-1.0</p> <p>Detected Licenses:</p> <p>Apache-2.0 (exemplary link to the first of 3 locations) EPL-1.0 (exemplary link to the first of 4 locations) EPL-2.0 (link to the location) NOASSERTION (link to the location)</p>		
3	Maven:org.hamcrest:hamcrest-core:1.3	test	<p>Declared Licenses:</p> <p>BSD-3-Clause</p>		
4	Maven:org.mockito:mockito-all:1.10.19	test	<p>Declared Licenses:</p> <p>MIT</p> <p>Detected Licenses:</p> <p>Apache-2.0 (exemplary link to the first of 123 locations) BSD-3-Clause (exemplary link to the first of 89 locations) MIT (exemplary link to the first of 336 locations)</p>		

<https://github.com/junit-team/junit/tree/r4.12/src/site/fml/faq.fml#L156>

© Bosch.IO GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution as well as in the event of applications for industrial property rights.

Case 5: Curation Team - issue

For demonstration: scan-result.yml manipulated => deleted the license declaration for junit to pretend it would be missing

Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T12:39:34.870956900Z.

Project

Scanned revision 7653e418d610ffd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index

[Rule Violation Summary \(3 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Rule Violation Summary (3 errors, 0 warnings, 0 hints to resolve)

#	Rule	Package	License	Message
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DETECTED: EPL-1.0	The ScanCode copyleft-limited categorized license EPL-1.0 was detected in package Maven:junit:junit:4.12. How to fix
2	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	DETECTED: EPL-2.0	The ScanCode copyleft-limited categorized license EPL-2.0 was detected in package Maven:junit:junit:4.12. How to fix
3	UNHANDLED_LICENSE	Maven:junit:junit:4.12	DETECTED: NOASSERTION	The license NOASSERTION is currently not covered by policy rules. The license was detected in package Maven:junit:junit:4.12 How to fix

ISSUE for the Curation Team:
Component with no declared but only detected licenses
=> Curation Team needs to investigate the situation

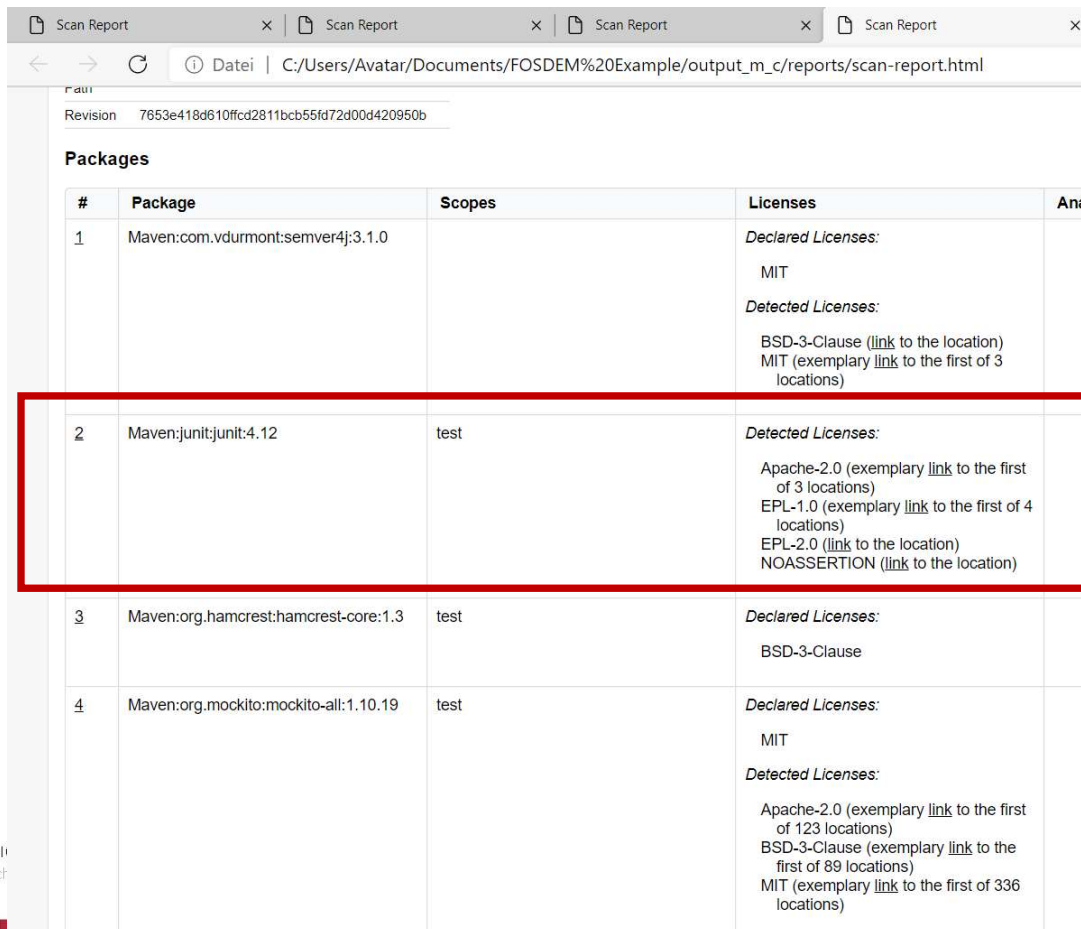
Bosch
© Bos

BOSCH

Case 5: Curation Team - issue

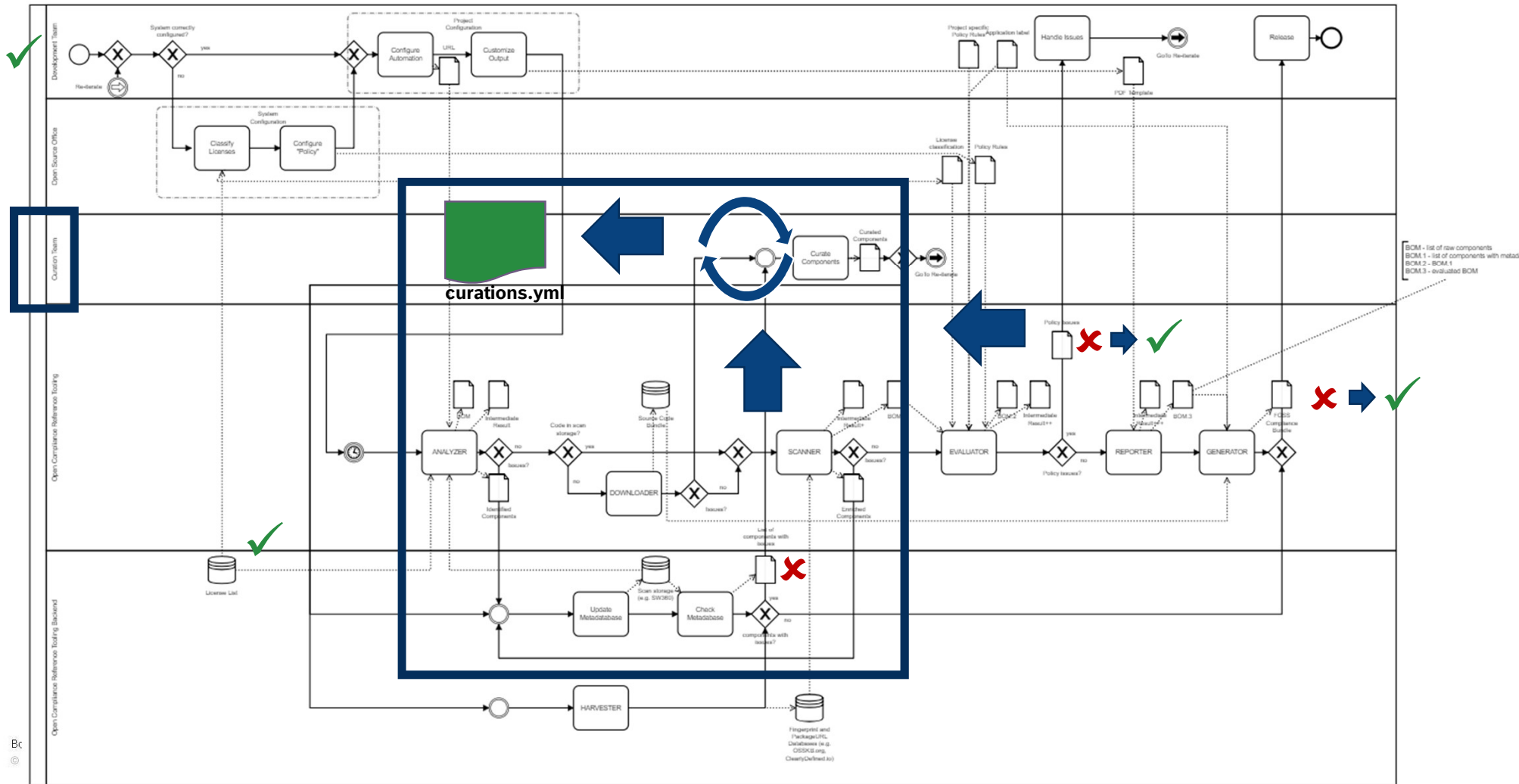
For demonstration: scan-result.yml manipulated => deleted the license declaration for junit to pretend it would be missing

ISSUE for the Curation Team: Component with no declared but only detected licenses => Curation Team needs to investigate the situation, the result may be globally provided in the curations.yml in the ort-config-folder or as project specific resolution or curation in the .ort.yml in the project repository root folder.



#	Package	Scopes	Licenses	Anal
1	Maven:com.vdurmont:semver4j:3.1.0		Declared Licenses: MIT Detected Licenses: BSD-3-Clause (link to the location) MIT (exemplary link to the first of 3 locations)	
2	Maven:junit:junit:4.12	test	Detected Licenses: Apache-2.0 (exemplary link to the first of 3 locations) EPL-1.0 (exemplary link to the first of 4 locations) EPL-2.0 (link to the location) NOASSERTION (link to the location)	
3	Maven:org.hamcrest:hamcrest-core:1.3	test	Declared Licenses: BSD-3-Clause	
4	Maven:org.mockito:mockito-all:1.10.19	test	Declared Licenses: MIT Detected Licenses: Apache-2.0 (exemplary link to the first of 123 locations) BSD-3-Clause (exemplary link to the first of 89 locations) MIT (exemplary link to the first of 336 locations)	

Case 5: Curation Team issue



Folder: [Software Repository/ INST/ INST Checks/ junit4-r4.12.zip/junit4-r4.12](#)

[License Browser](#) |
 [File Browser](#) |
 [Copyright](#) |
 [ECC](#) |
 [Email/URL/Author](#) |
 [Keyword](#) |
 [Browse](#) |
 [License List](#) |
 [Search](#) •
 [View](#) |
 [Conf](#) |
 [Info](#)

Display licenses

Scanner Count	Concluded License Count	License Name
4	0	EPL-1.0
4	0	CPL
2	0	Apache-2.0
1	0	BSD-3-Clause

Showing 1 to 4 of 4 licenses

Page of 1

Hint: Click on the license name to search for where the license is found in the file listing.

Summary

Unique licenses	4	565	Files
Unique scanner detected licenses	5	0	Unique concluded licenses
Licenses found	11	0	Licenses concluded
Files with no detected licenses	554	0	Concluded files with no detected licenses

Display files (tree view or flat)

	EPL-1.0	-- filter for edited results --	<input type="checkbox"/> open		MarkAsI
Files	Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport, O: ojo)	Edited Results	Clearing Status	Files Cleared	Actions
src	Apache-2.0, EPL-1.0, No_license_found		●	0/3	[Tag][Edit]
epl-v10.html	EPL-1.0 [N][M: 87%]		●	0/1	[View][Ir][Downloa][Edit]
LICENSE-junit.txt	EPL-1.0 [N][M: 99%]		●	0/1	[View][Ir][Downloa][Edit]
pom.xml	EPL-1.0 [N]		●	0/1	[View][Ir][Downloa][Edit]

Showing 1 to 4 of 4 files (filtered from 19 total entries)

Page

Open Compliance Reference Tooling

Sharing the metadata...

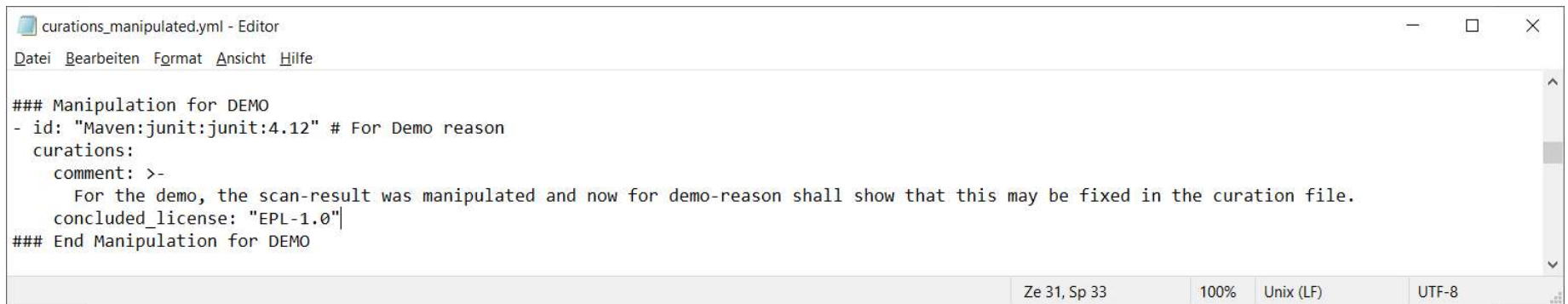


- ▶ The curations in the tool may be shared with ClearlyDefined if configured accordingly
- ▶ This way it is also possible to benefit from curations that were already shared in the community and reduce the effort



- ▶ <https://clearlydefined.io>

Case 5: Curation Team - issue



```
curations_manipulated.yml - Editor
Datei Bearbeiten Format Ansicht Hilfe

### Manipulation for DEMO
- id: "Maven:junit:junit:4.12" # For Demo reason
  curations:
    comment: >-
      For the demo, the scan-result was manipulated and now for demo-reason shall show that this may be fixed in the curation file.
    concluded_license: "EPL-1.0"
### End Manipulation for DEMO

Ze 31, Sp 33 100% Unix (LF) UTF-8
```

Case 5: Curation Team - issue

Scan Report

Scan Report

Scan Report

Scan Report

ort/config-file-curations.yml

Scan Report

C:/Users/Avatar/Documents/FOSDEM%20Example/output_m_c/reports/scan-report.html

Scan Report

Created by **ORT**, the [OSS Review Toolkit](#), version f5a1d22 on 2021-01-24T13:27:23.579054Z.

Project
Scanned revision 7653e418d610ffd2811bcb55fd72d00d420950b of Git repository <https://github.com/vdurmont/semver4j.git>

Index
[Rule Violation Summary \(1 errors, 0 warnings, 0 hints to resolve\)](#)
[Maven:com.vdurmont:semver4j:3.1.0](#)
[Repository Configuration](#)

Rule Violation Summary (1 errors, 0 warnings, 0 hints to resolve)

#	Rule	Package	License	Message
1	COPYLEFT_LIMITED_IN_SOURCE	Maven:junit:junit:4.12	CONCLUDED: EPL-1.0	<div>The package Maven:junit:junit:4.12 has the concluded ScanCode copyleft-limited categorized license EPL-1.0.</div> <div>► How to fix</div>

Maven:com.vdurmont:semver4j:3.1.0 (pom.xml)
VCS Information

Type	Git
URL	https://github.com/vdurmont/semver4j.git
Path	
Revision	7653e418d610ffd2811bcb55fd72d00d420950b

Packages

B
C

BOSCH

Case 5: Curation Team - issue

Revision: 7055c470dd70f1c0a2071b0b330d72d00d420550b					
Packages					
#	Package	Scopes	Licenses	Analyzer Issues	Scanner Issues
1	Maven:com.vdurmont:semver4j:3.1.0		Declared Licenses: MIT Detected Licenses: BSD-3-Clause (link to the location) MIT (exemplary link to the first of 3 locations)		
2	Maven:junit:junit:4.12	test	Concluded License: EPL-1.0 Detected Licenses: Apache-2.0 (exemplary link to the first of 3 locations) EPL-1.0 (exemplary link to the first of 4 locations) EPL-2.0 (link to the location) NOASSERTION (link to the location)		
3	Maven:org.hamcrest:hamcrest-core:1.3	test	Declared Licenses: BSD-3-Clause		
4	Maven:org.mockito:mockito-all:1.10.19	test	Declared Licenses: MIT		

THANK YOU!



Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: <https://groups.io/g/oss-based-compliance-tooling>

Online meetings: Bi-weekly -Invitations are sent to the mailing list

Website: [https://oss-compliance-tooling.org /](https://oss-compliance-tooling.org/)

And of course we are on GitHub:

<https://github.com/Open-Source-Compliance/Sharing-creates-value>