

Open Source Summit Japan

Thursday July 18, 2019 ~~16:50 - 17:30~~ 16:00 - 16:40

Hall B (4)

# Using SW360 for OSS Compliance Management Process

**TOSHIBA**

Kouki Hama [kouki1.hama@toshiba.co.jp](mailto:kouki1.hama@toshiba.co.jp)

Software Engineering & technology center

Open Source Technology Department

**Thursday July 18, 2019 16:50 - 17:30**

**Hall B (4)**  
**Open Source Leadership**

**Experience Level Beginner**

**<https://events.linuxfoundation.jp/events/open-source-summit-japan-2019/program/schedule/>**

## Summary

SW360 is an OSS tool used for centrally managing software component information, license information, vulnerability information, and etc. This tool also allows you to associate project information with many software components.

Toshiba has begun centralizing information management of open source software by SW360. This made it possible to share open source information across departmental barriers. On the other hand, feedback from users obtained various issues.

Kouki will explain how Toshiba has promoted the use of open source by SW360 and will explain how to approach issues. These include issues that originate from Japan domestic requirement and issues that need to be solved beyond the boundaries of a company. Moreover, Kouki will report on what kind of open source compliance management system Toshiba aims for.

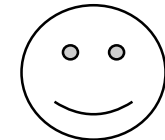
# Who am I ?

Kouki Hama (濱 功樹)

- Toshiba Corporation (2016~now)
- Research and Development OSS Compliance / Management Tool
  - SW360, Fossology, GitLab, spdx tool, ...
- Hobby
  - Playing with my cats
  - Mathematics (Research Nonlinear Optimization Algorithm)
  - Pokémon Go



Hi I am Hama

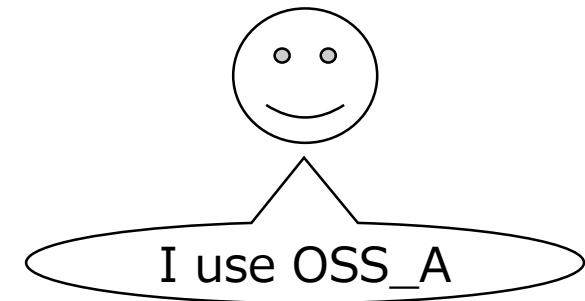
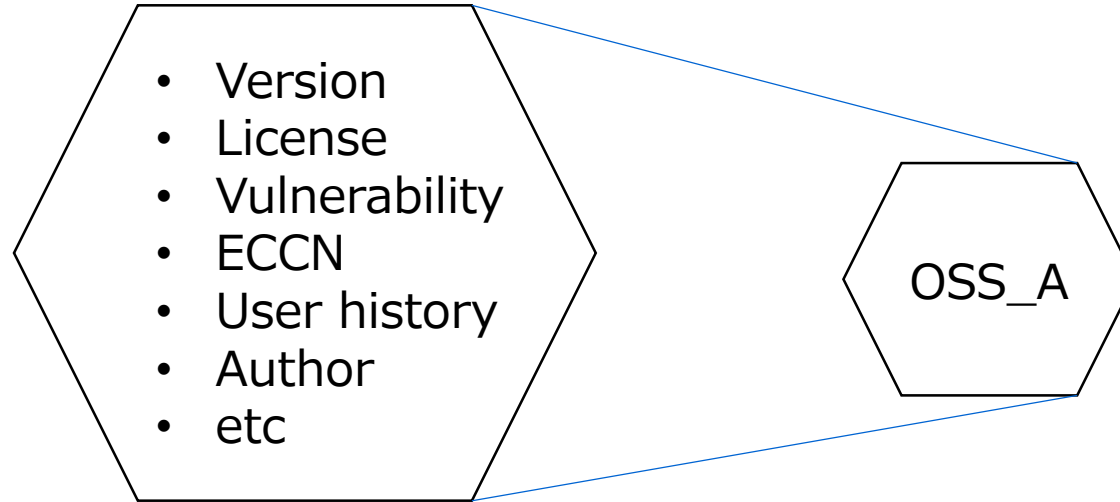


## Today's presentation consists of 5 points

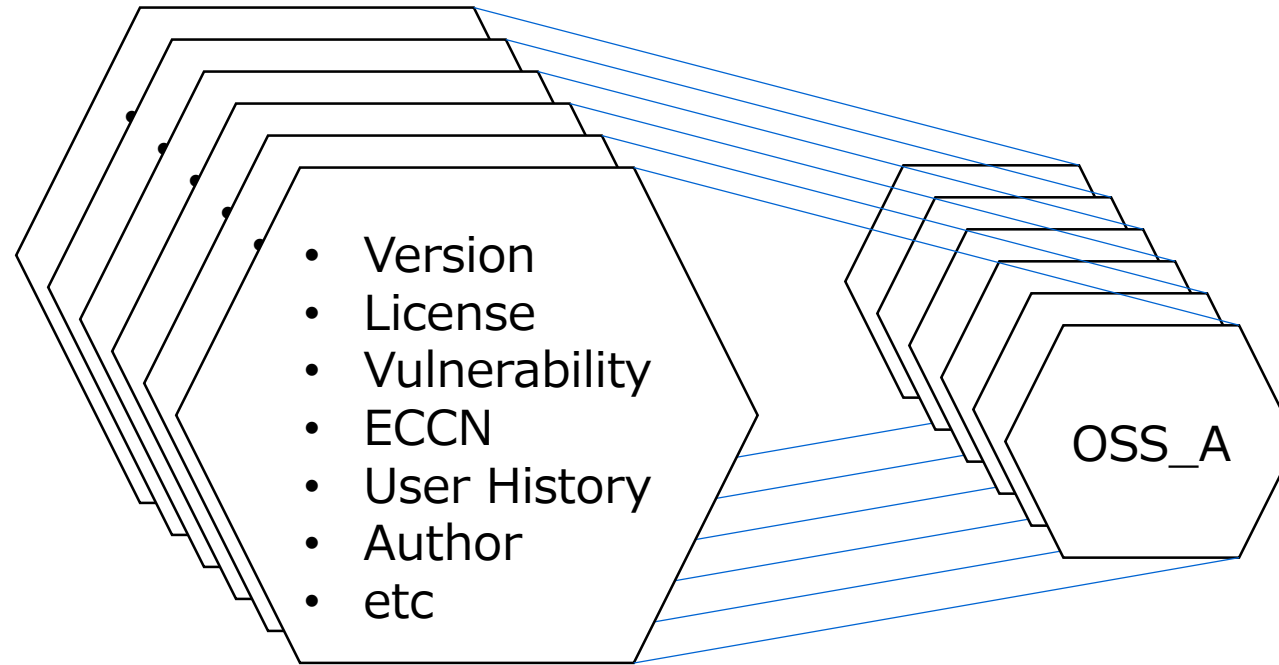
- Difficulty of Open Source Software compliance management
- How to manage OSS with SW360 property ?
- OSS SW360 Ecosystem
- Live demonstration
- Q & A

## Difficulty of Open Source Software compliance management

# Need to confirm a lot of OSS information before Using OSS

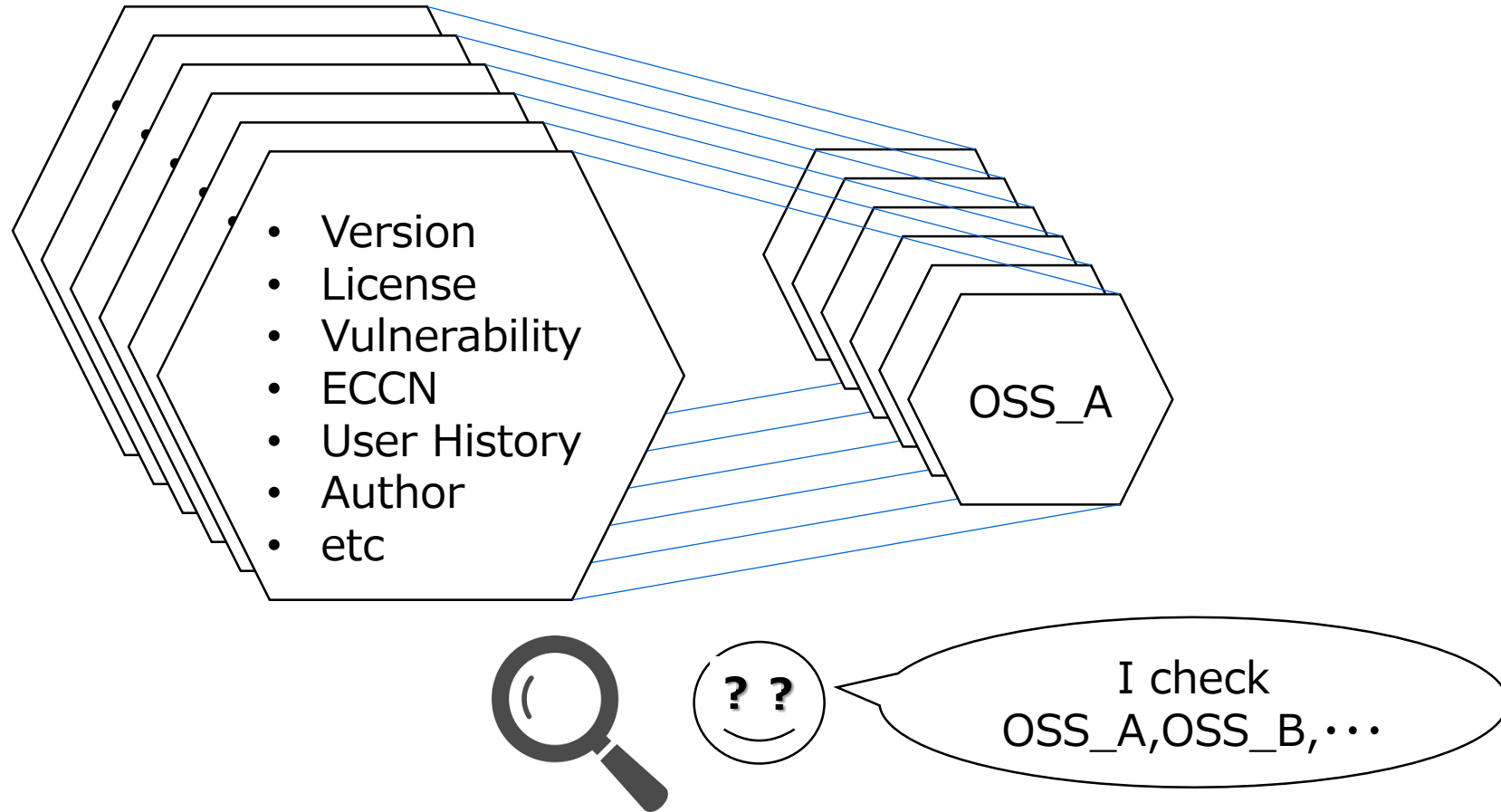


# OSS spreading like mushrooms around the world

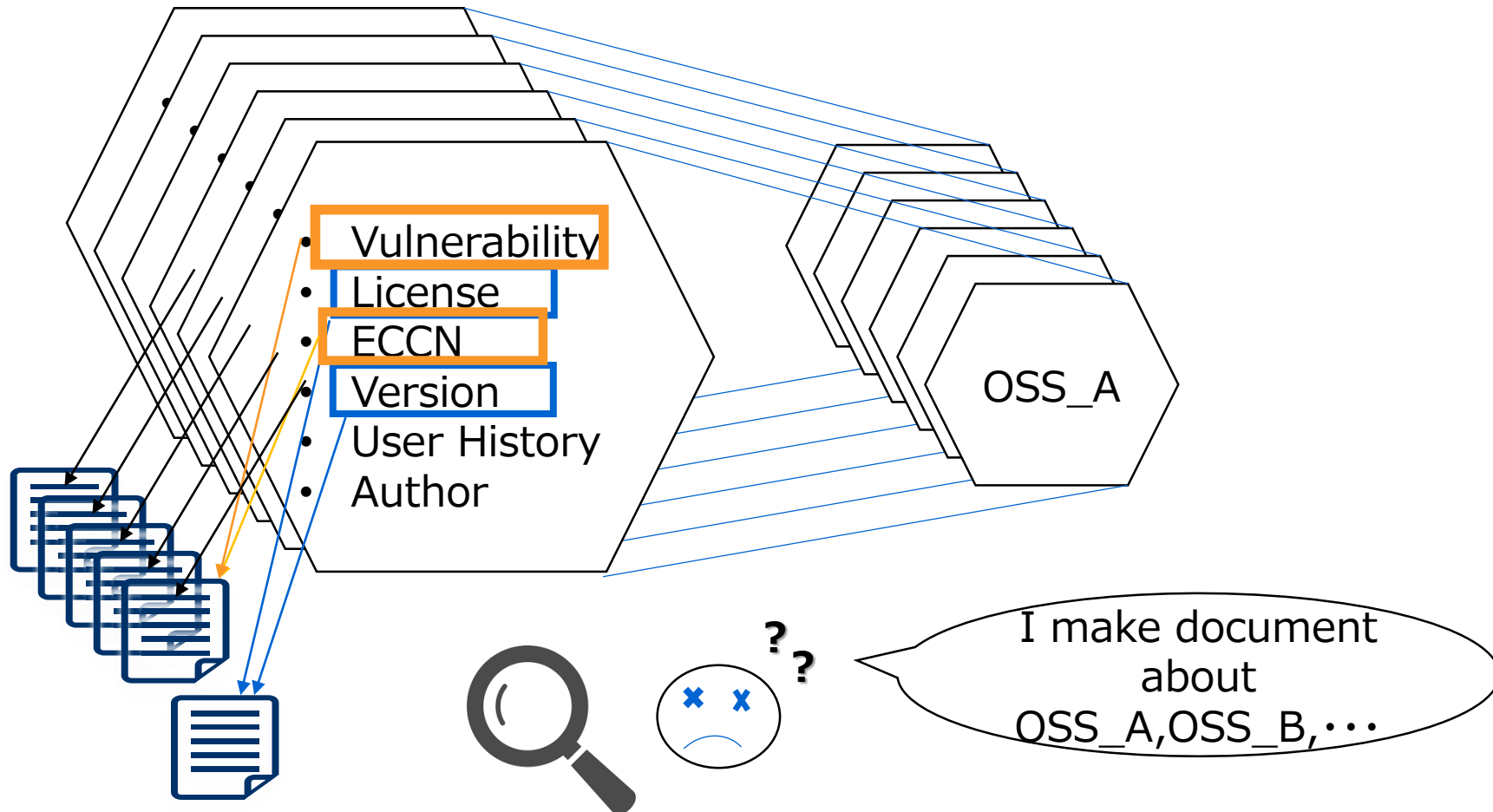




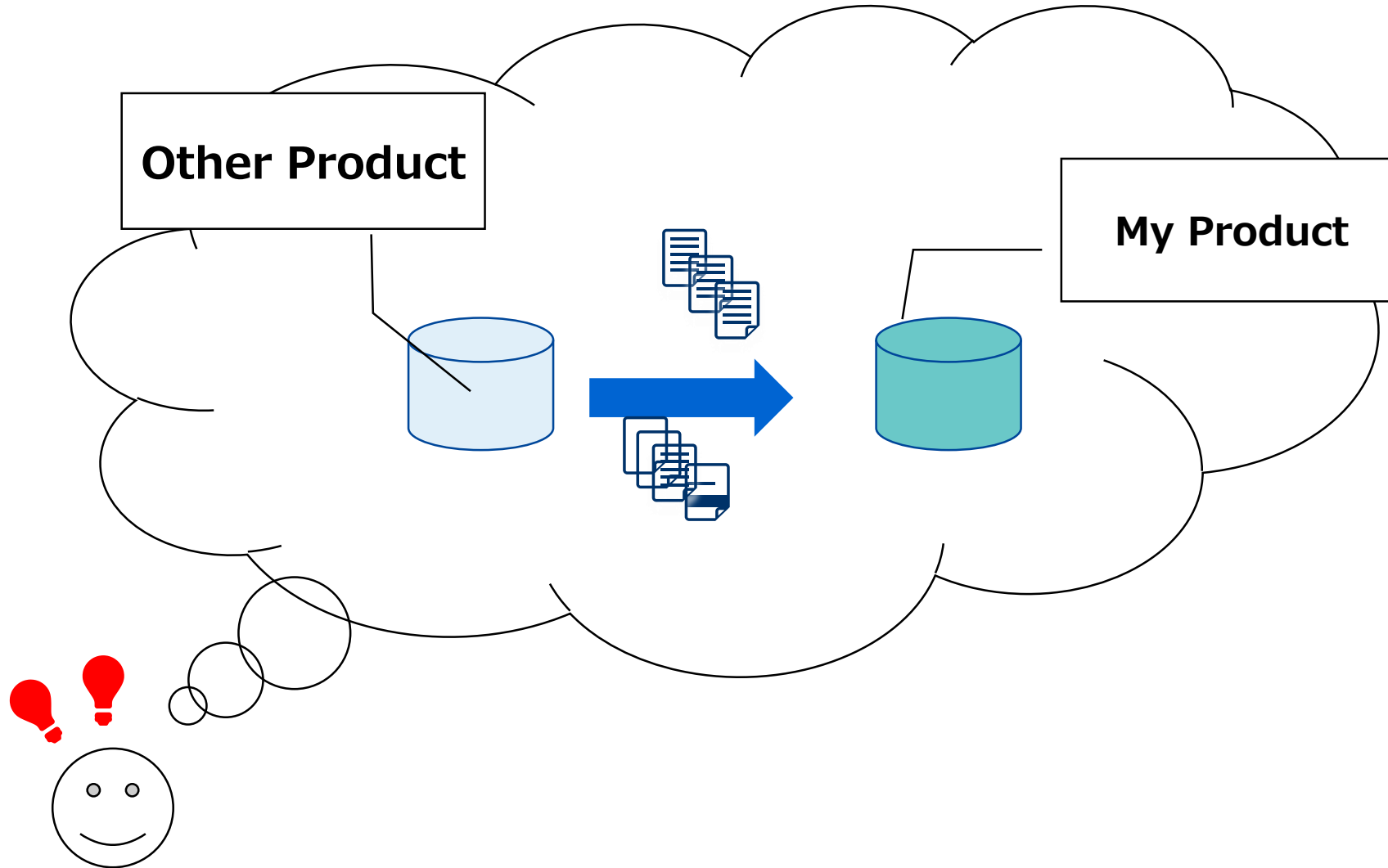
# And we need to clarify a lot of OSS related information



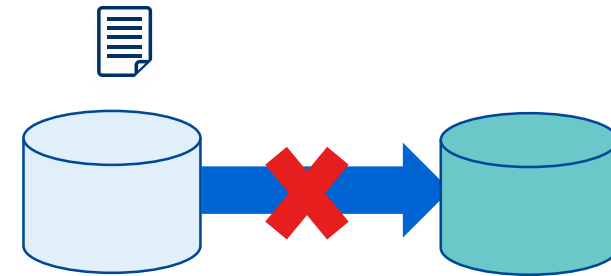
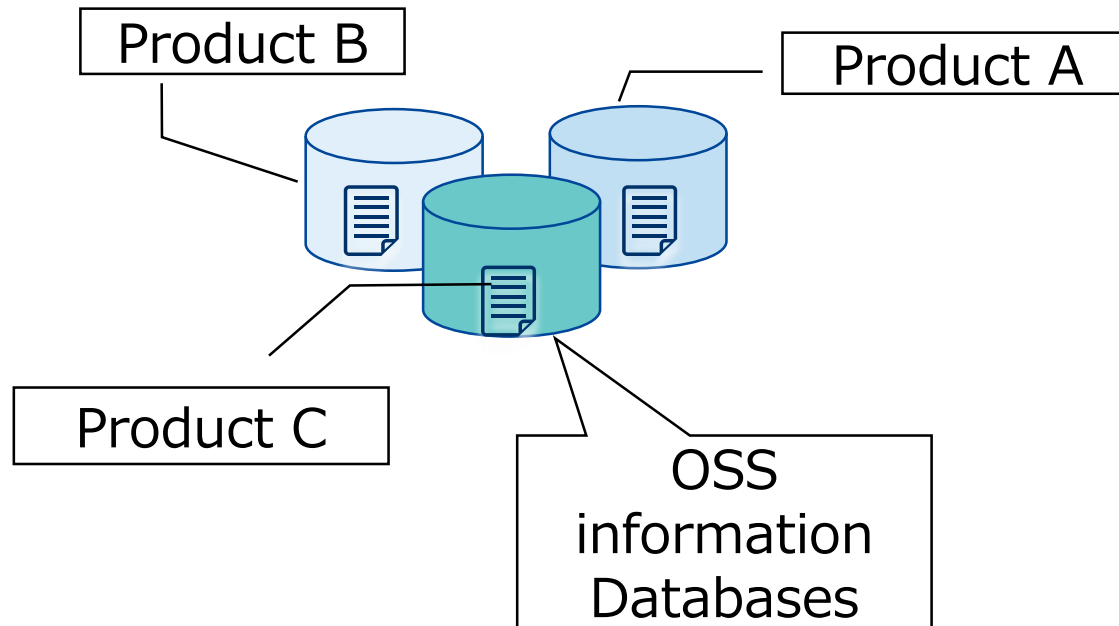
# In addition we need to prepare a lot of OSS related documents



# Occasionally, Reusing other department/product's OSS related documentation should look good



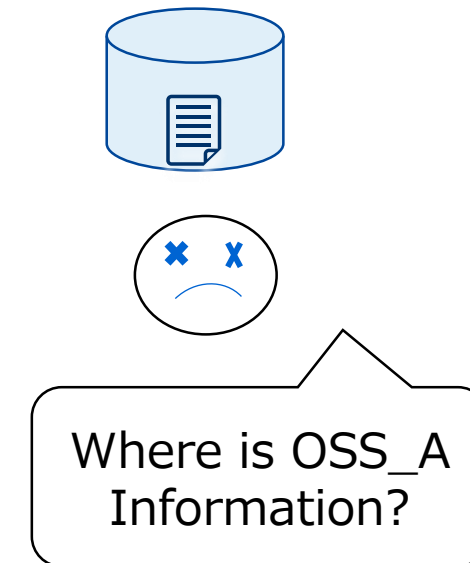
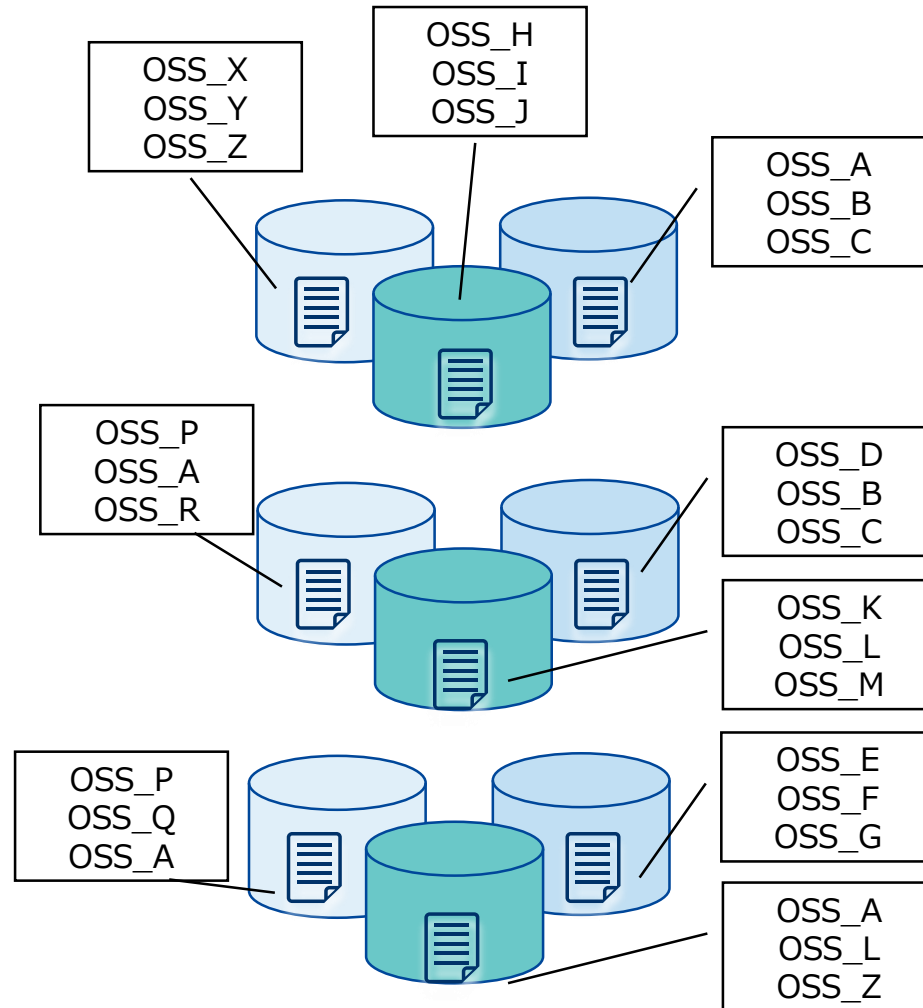
# However, reusing other product/project OSS information is challenging



WHY?

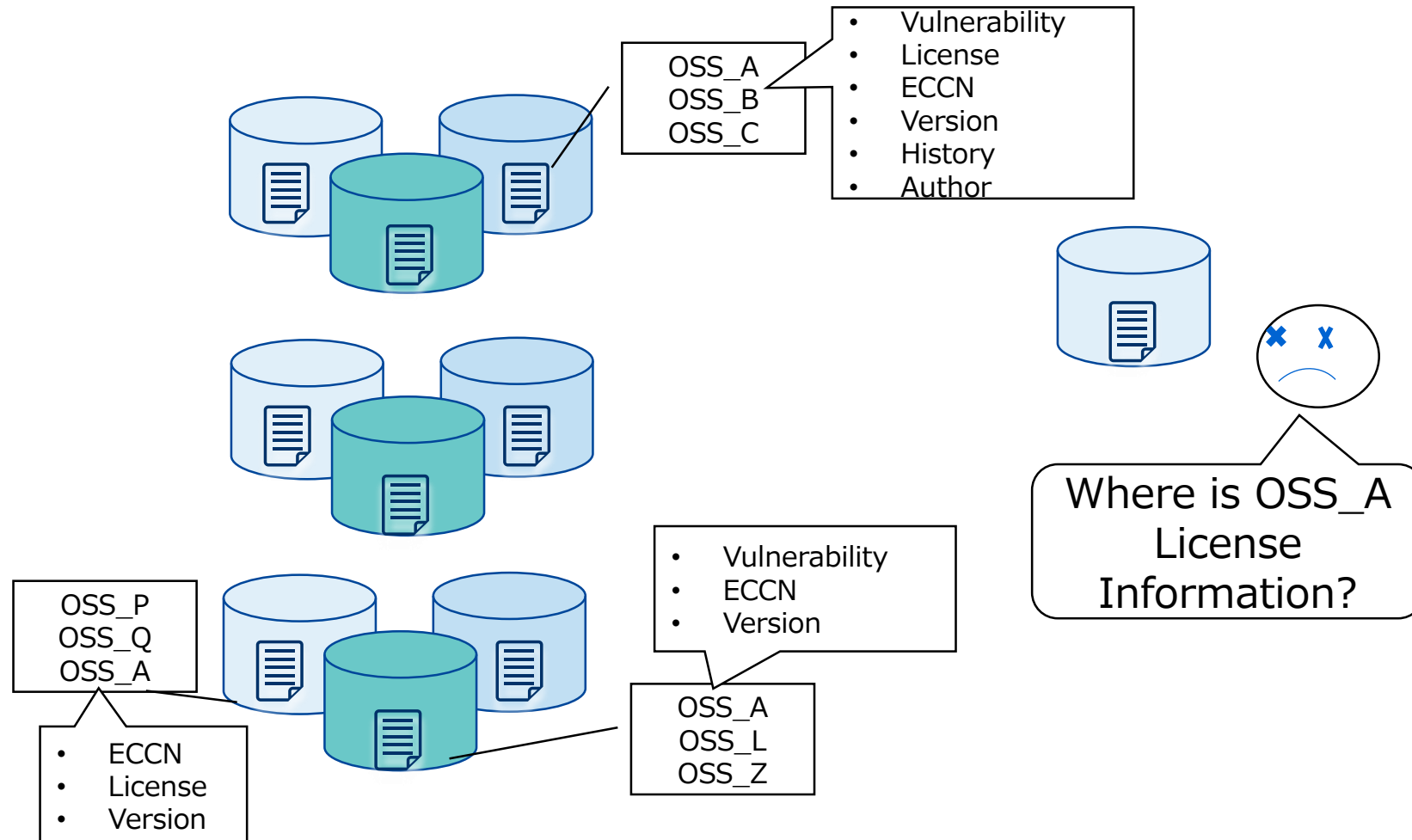
# Answer 1.

Finding property information from a lot of other products is tedious



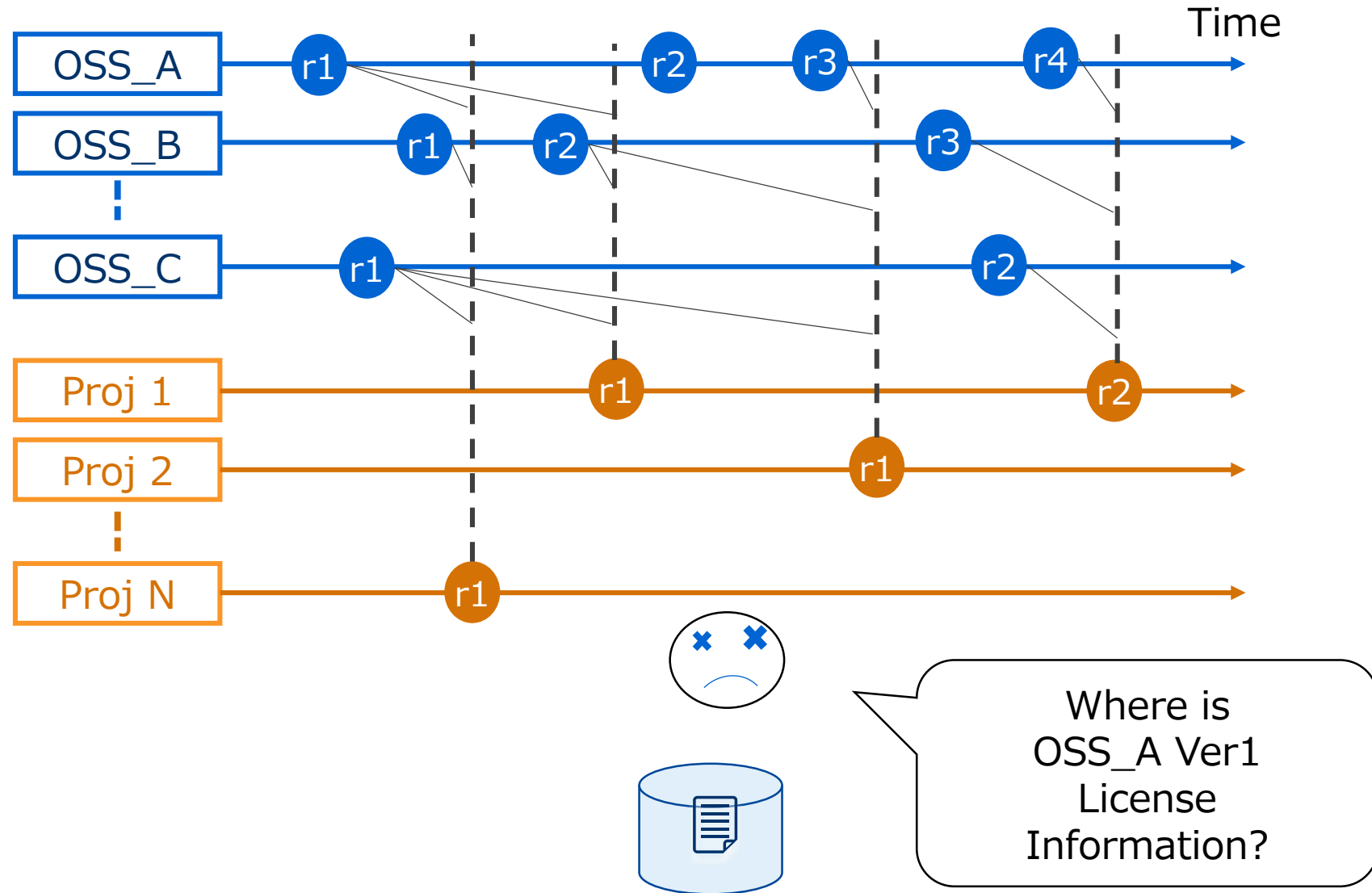
## Answer 2.

Different products have their own respective OSS information



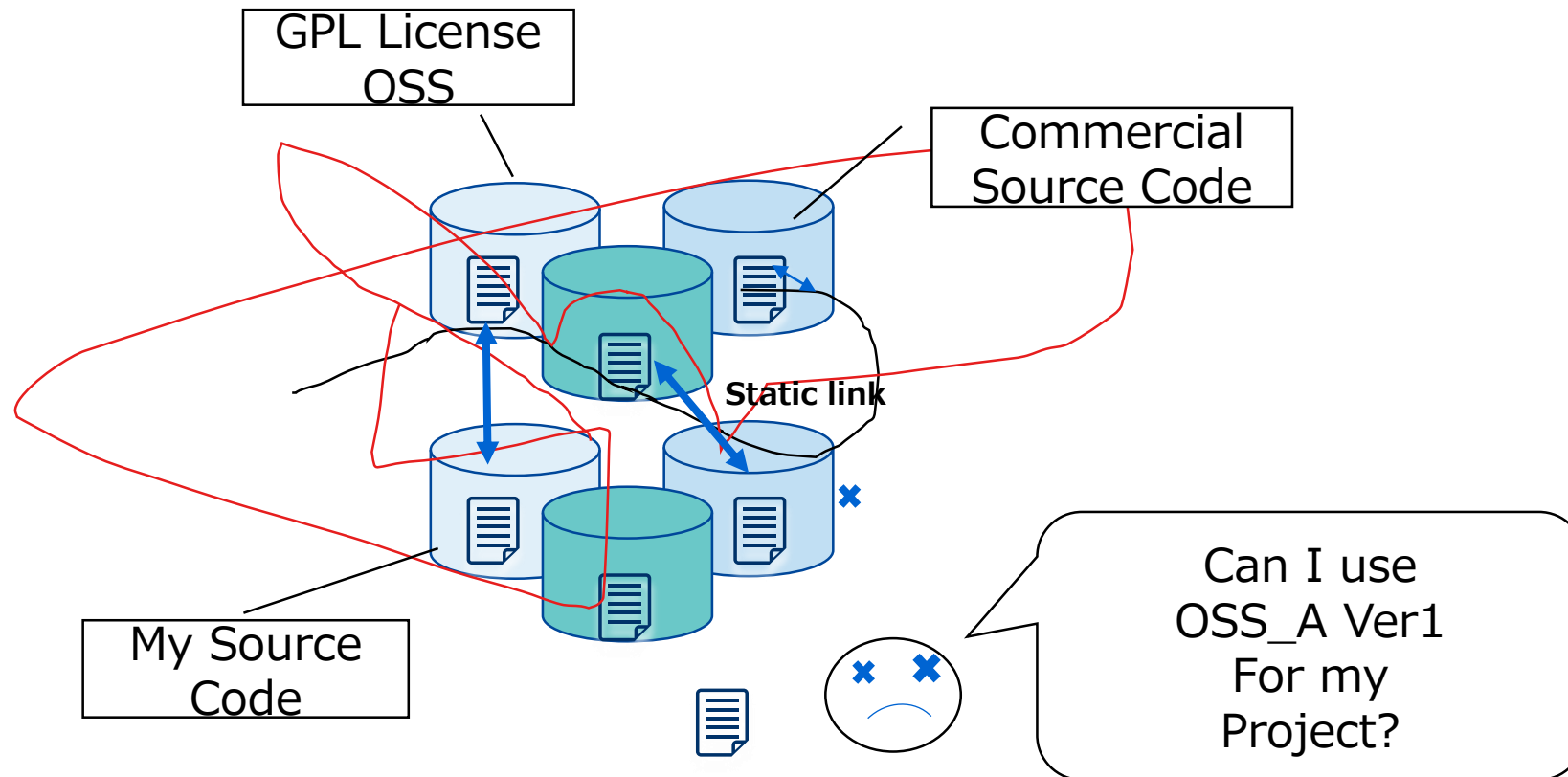
### Answer 3.

Different products have unique OSS version information.



Moreover

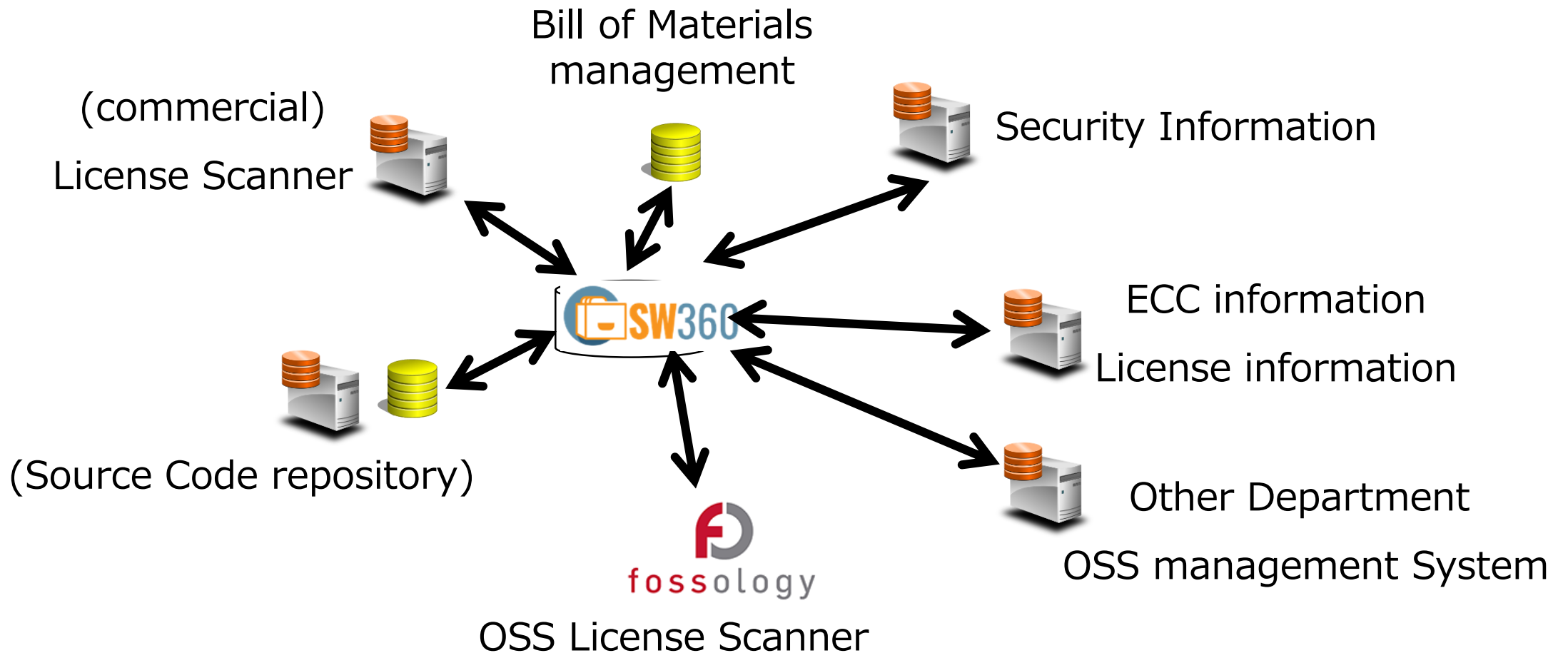
**Software dependency is a significant factor,  
however can be complex.**





# We need put together OSS information

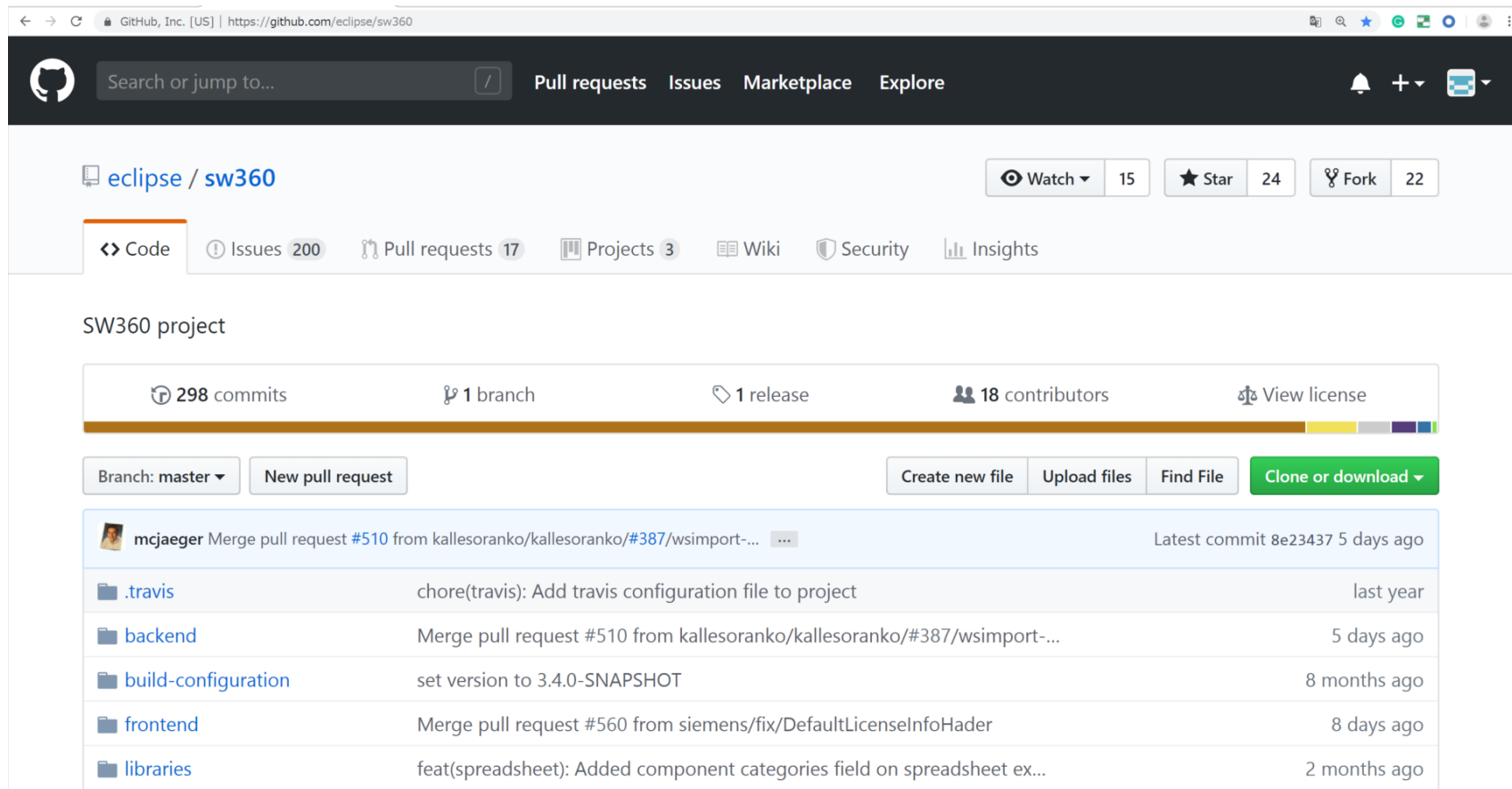
- OSS review requires a certain amount of time
- Avoid checking the same OSS information numerous times



# The best approach is Utilizing the OSS compliance tool.



<https://github.com/eclipse/sw360>

A screenshot of the GitHub repository page for eclipse/sw360. The page shows the repository name, navigation tabs (Code, Issues, Pull requests, Projects, Wiki, Security, Insights), and a list of recent commits. The commits list includes details like the author (mcjaeger), the commit message, and the time since the commit.

GitHub, Inc. [US] | <https://github.com/eclipse/sw360>

Search or jump to... Pull requests Issues Marketplace Explore

eclipse / sw360 Watch 15 Star 24 Fork 22

Code Issues 200 Pull requests 17 Projects 3 Wiki Security Insights

SW360 project

298 commits 1 branch 1 release 18 contributors View license

Branch: master New pull request Create new file Upload files Find File Clone or download

mcjaeger Merge pull request #510 from kallesoranko/kallesoranko/#387/wsimport-... Latest commit 8e23437 5 days ago

.travis	chore(travis): Add travis configuration file to project	last year
backend	Merge pull request #510 from kallesoranko/kallesoranko/#387/wsimport-...	5 days ago
build-configuration	set version to 3.4.0-SNAPSHOT	8 months ago
frontend	Merge pull request #560 from siemens/fix/DefaultLicenseInfoHader	8 days ago
libraries	feat(spreadsheet): Added component categories field on spreadsheet ex...	2 months ago

# What is SW360 ?

<https://github.com/eclipse/sw360>

A software component catalogue application –  
designed to work with FOSSology.



# SW360 Management and Associate Project Information With OSS related Component

General

Name *	Version	Project visibility *
<input type="text"/>	<input type="text"/>	Group and Moderators ▼
Created by	HomePage URL	Wiki URL
<input type="text"/>	<input type="text"/>	<input type="text"/>
Project type *	Tag	Description
Customer Project ▼	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Enable Security Vulnerability Monitoring	<input type="checkbox"/> Enable Displaying Vulnerabilities	

Roles

Group *	Project manager	Project owner
<input type="text"/>	<input type="text"/>	<input type="text"/>
Owner accounting unit	Owner billing group	Owner country
<input type="text"/>	<input type="text"/>	<input type="text"/>
Lead architect	Moderators	Contributors
<input type="text"/>	<input type="text"/>	<input type="text"/>
Security Responsibilities		
<input type="text"/>		
Additional Roles		
<input type="text"/>		
External Ids		
<input type="text"/>		

Project register snapshot

Name, Version,  
Project visibility, Project type,  
Group, Project owner, etc  
Project visibility, Project type,  
Group, Project owner, etc

Edit

Delete 0testjavascript-common (0.0.0)

Release Summary

Vendor	Name *	Version *
<input type="text"/>	0testjavascript-common	0.0.0
Programming Languages	Operating Systems	CPE ID
<input type="text"/>	<input type="text"/>	cpe:2.3:...:apache:"maven.*" ▼
Release Date	Licenses	Download URL
<input type="text"/>	GPL-2.0+	<input type="text"/>
Clearing State	Release Mainline State	Created on
<input type="text"/>	Mainline ▼	2018/09/21
Created by	Contributors	Moderators
Kouki Hama	<input type="text"/>	<input type="text"/>
Additional Roles		
<input type="text"/>		
External Ids		
<input type="text"/>		
Release Repository	Repository Type	Repository URL
<input type="text"/>	Unknown ▼	<input type="text"/>

Component register snapshot

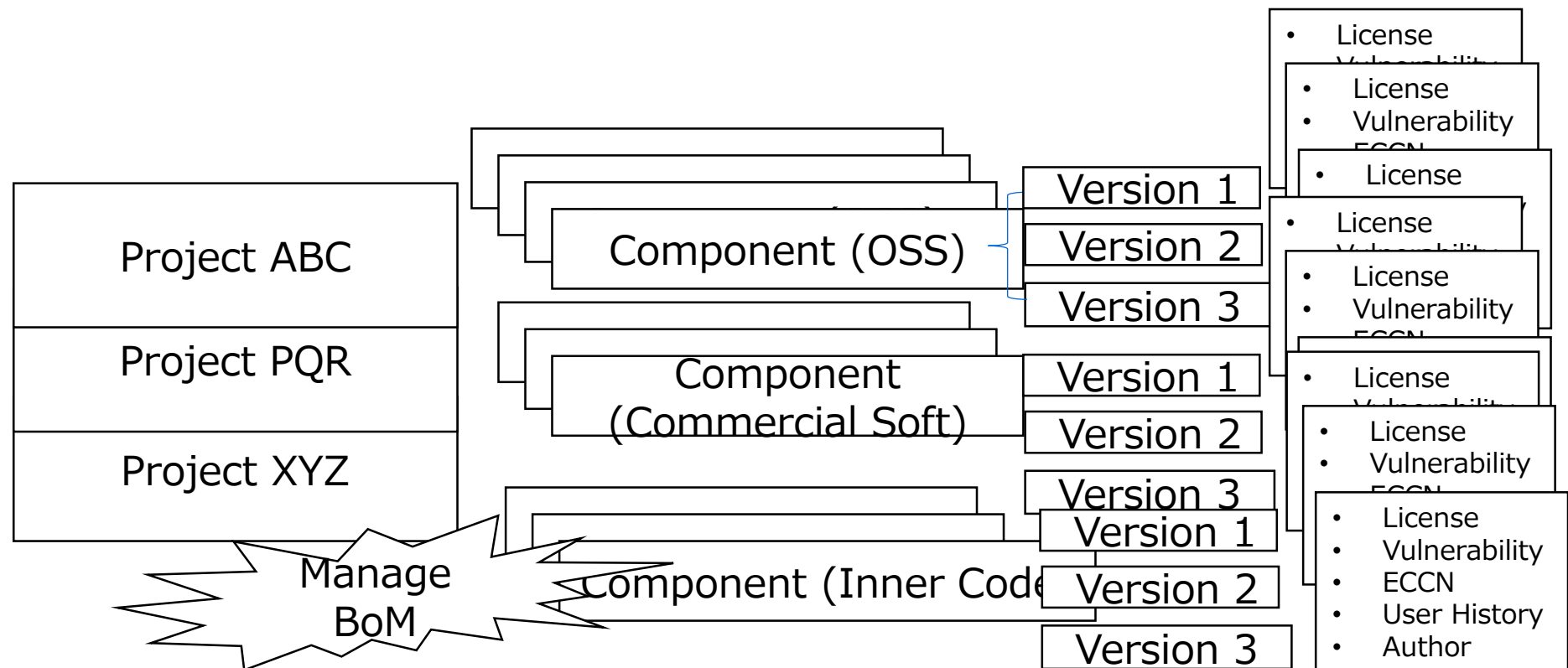
Name, Vendor, Version,  
Programming Languages,  
Operating System,  
Contributors, Download URL,  
License, CPE ID, etc

OSS Information

Linked each other

# You can also say that SW360 is the “Bill of Material” Management Tool

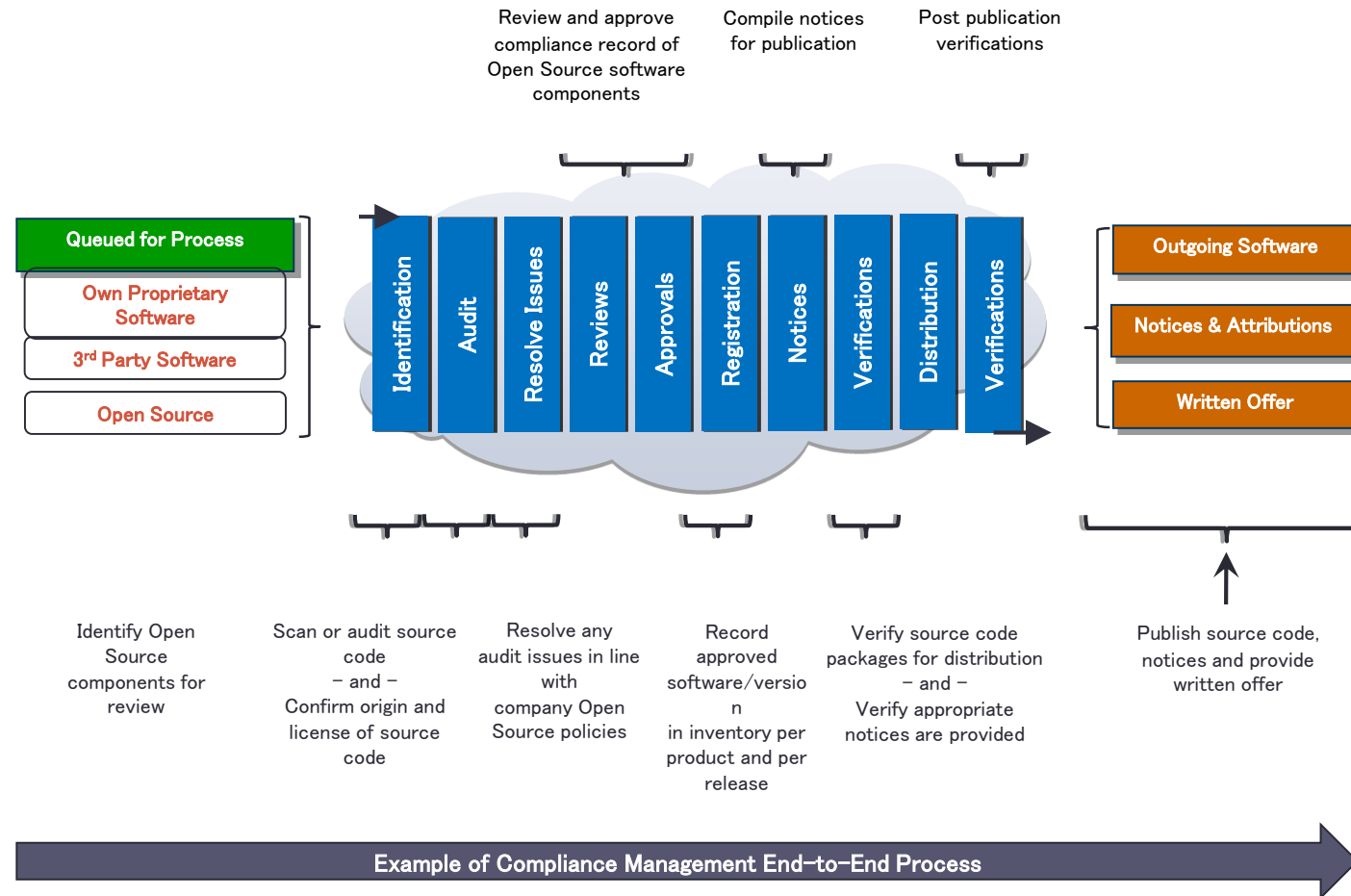
SW360 integrates all “Bill of Materials” in your company



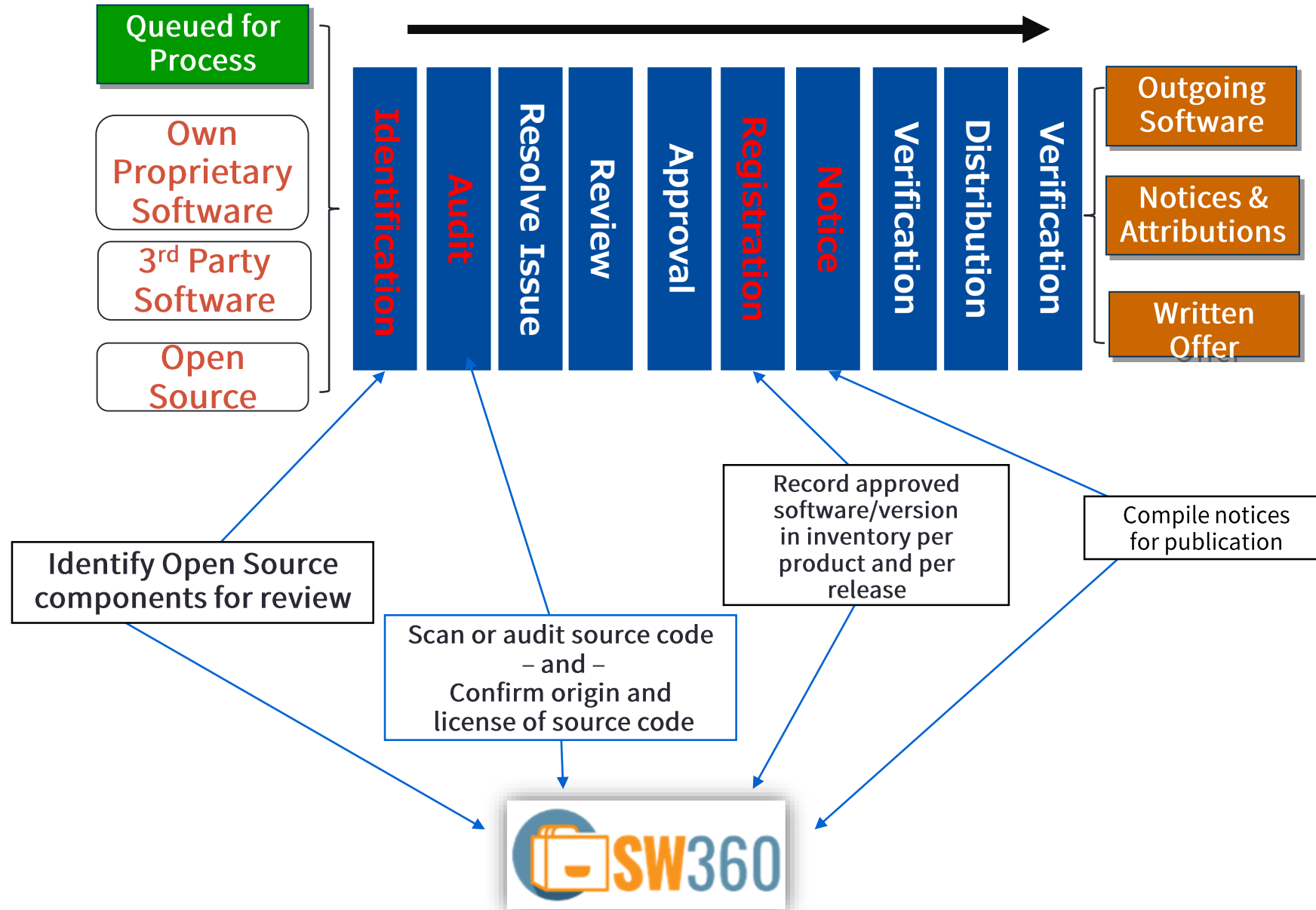
## How to manage OSS with SW360 property ?

Make it possible with  
OSS Management Process

# Example Enterprise Process



## SW360 assists OSS management



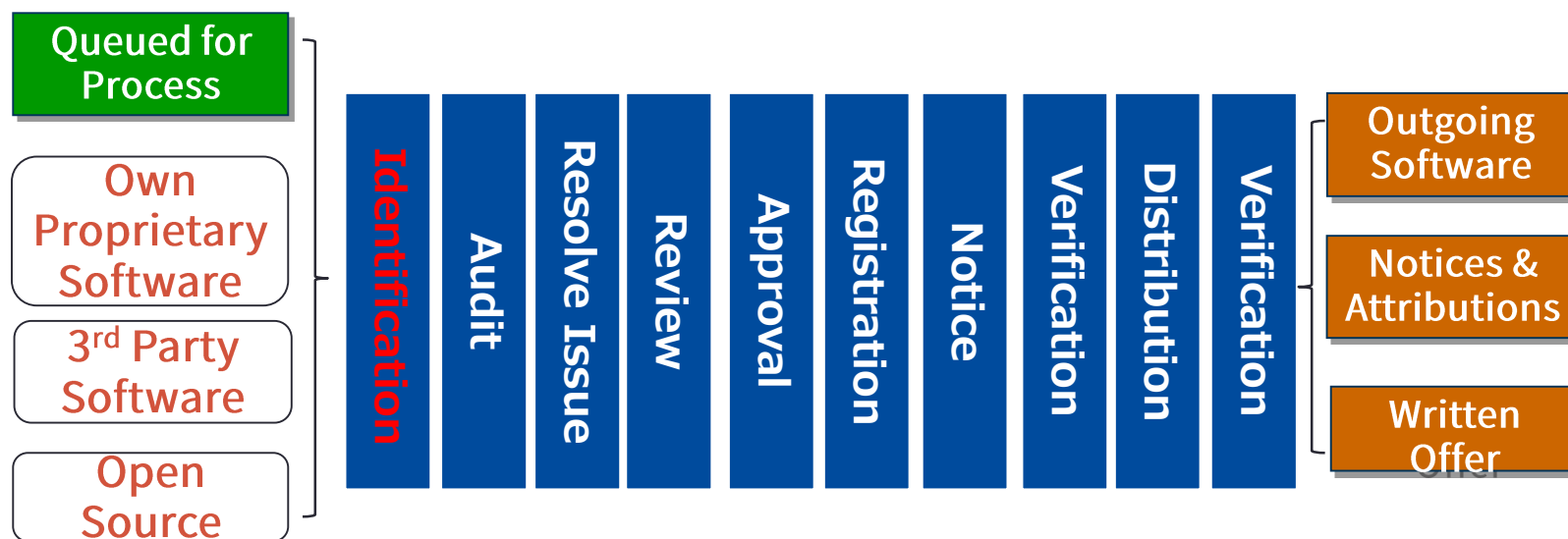


# Identification

Identify Open Source components for review

SW360 supports:

- ❑ Register to use OSS
- ❑ Search Used history of each OSS components



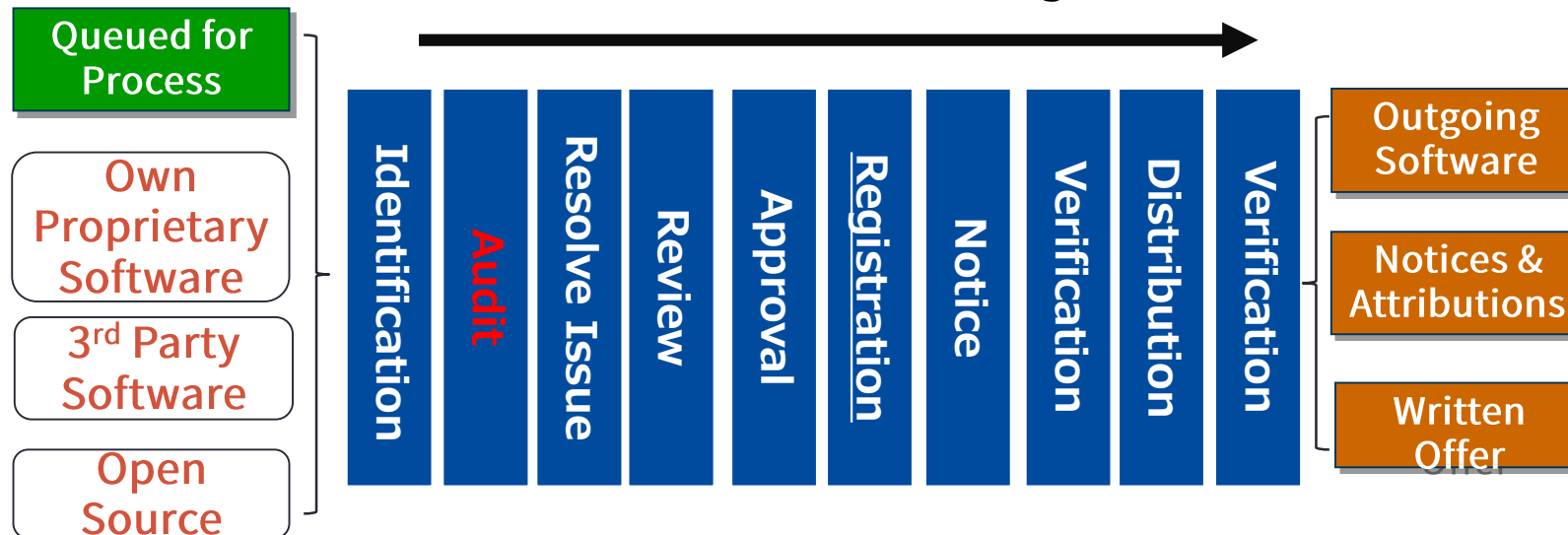
# Audit

Scan or audit source code – and –  
Confirm origin and license of source code

SW360 supports :

- ❑ Register OSS Source code (with version)
- ❑ License scan (License information from Fossology)
- ❑ Register CPE ID (For detecting Vulnerability)
- ❑ Register ECC (Export Control) Information

SW360 assists OSS management

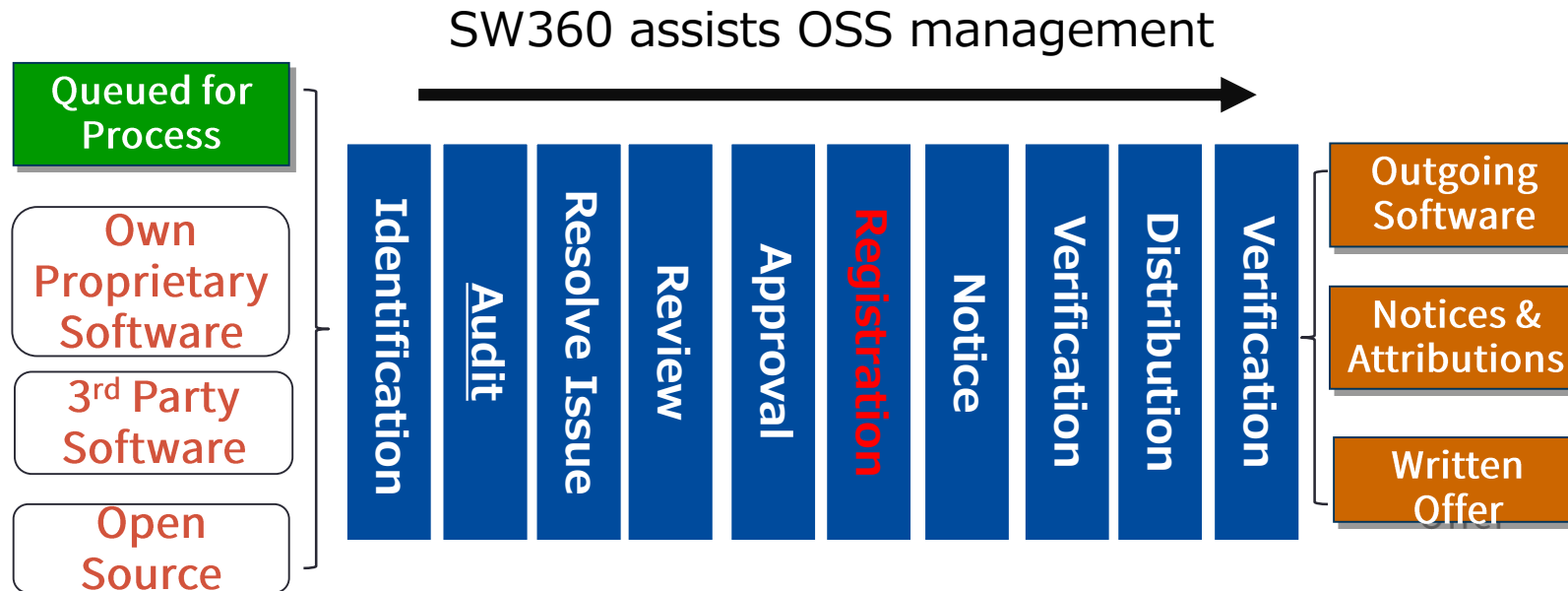


# Registration

Record approved software/version in inventory per product and per release

SW360 supports :

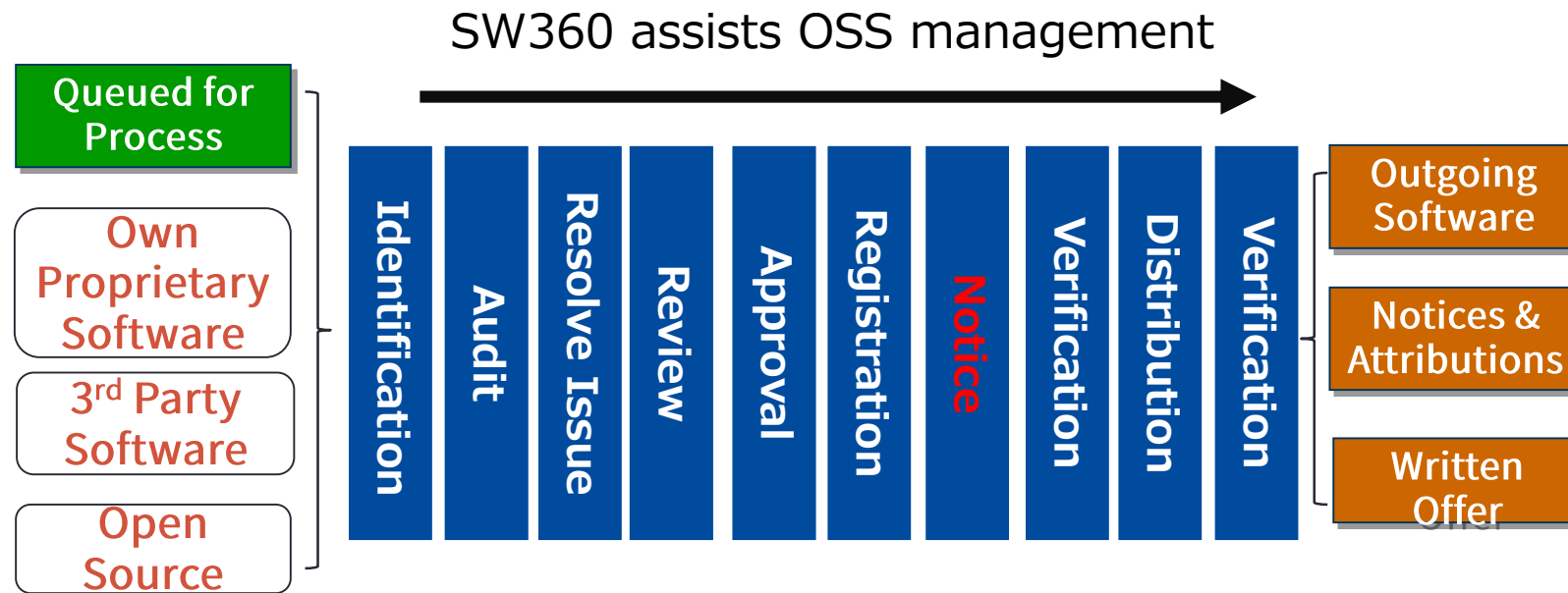
- ❑ Check OSS (Name, Version, Person in charge, etc.)  
And Projects (Name, Project Version, etc.)



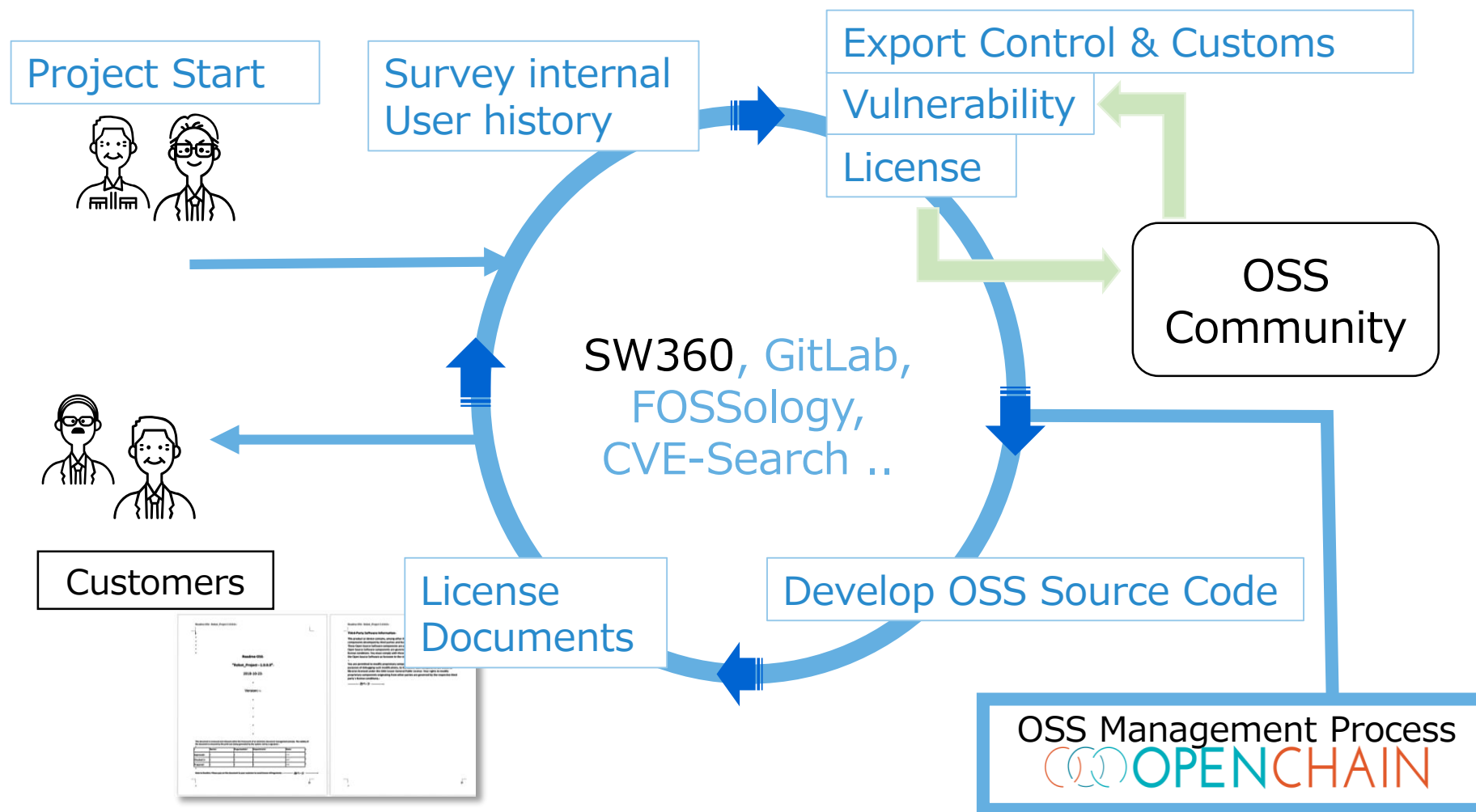
## Compile notices for publication

SW360 supports :

- ❑ Create user-friendly copyright and license list
- ❑ Register the format of the product attachment to be displayed on the document.



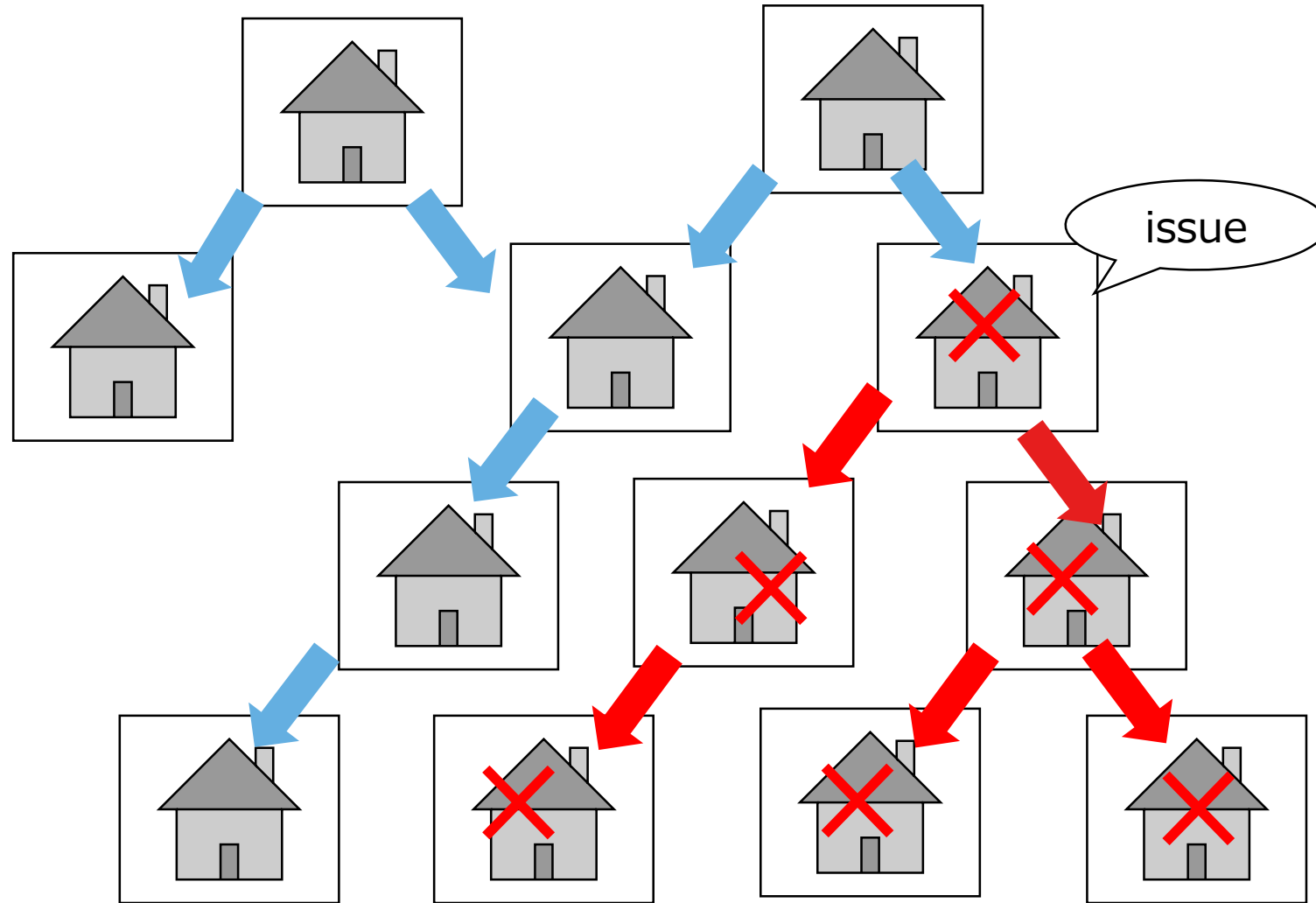
# TOSHIBA OSS Management System Goal !



Why do OSS related companies such as Toshiba need to utilize the OSS management system?



# One company's improper use of the OSS resonates throughout all the supply chain.



# TOSHIBA

## OSS SW360 Ecosystem



A lot of members will have access to discussions related to SW360 publicly.

- Open Chain Japan WG:

<https://wiki.linuxfoundation.org/openchain/openchain-japanese-working-group>

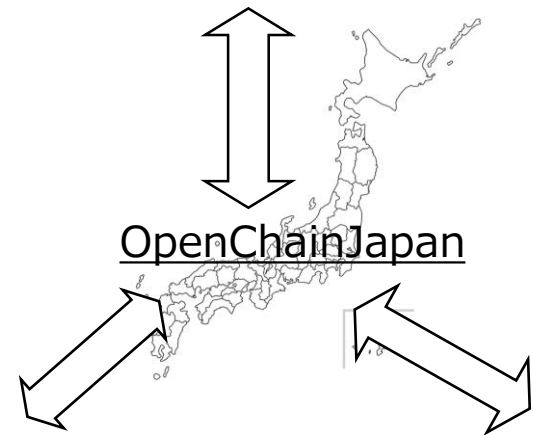
- OpenChain Tooling Work Group:

/ Sharing create values

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

# Open Chain Japan Work Group

- OpenChainJapan has Tooling Sub Group
- Try to discuss how to improve sw360's interface for non - English speakers / Japanese users.
  - Apply for Japanese vulnerability information
    - JVN = Japan Vulnerability Notes
  - Translate to Japanese language
    - Not only Japanese but also others
  - etc



Interpret in the Japanese language while sharing information with all OSS related connections in the world.

## In conclusion

- OSS management can be daunting
- Centering OSS information by SW360 is viable
- SW360 assists by complying with the OpenChain Process
- More people are showing interest in SW360

## Try SW360

I'm going to give a live demonstration on how to use SW360 Create Project information which includes component information

# Create Software Component

[Components]-[Add Component]

New Component

Add ComponentCancel

General

Name \*

Enter Name

Created by

Will be set automatically

Categories \*

e.g., Library,cloud,mobile,...

Component Type

OSS

Default vendor

Click to set vendor

Homepage URL

Enter Home Url

Blog URL

Enter Blog Url

Wiki URL

Enter Wiki Url

Mailing List URL

Enter Mailing List Url

Short Description

Enter Description

Roles

Component owner

Click to edit

Owner Accounting Unit

Enter Owner Accounting Unit

Owner Billing Group

Enter Owner Billing Group

SW360 | © Siemens AG 2013-2017, Bosch Software Innovations GmbH 2017 | Report an issue. | Version: 3.4.0-SNAPSHOT | Branch: master (cb4ad86) | Build time: 2019-06-13T10:46:34Z

# Register Component Release Information

Register Version etc...  
[Components]-[Edit]-[Add Release]

New Release

Test Component: New Release Edit

Summary

Linked Releases

Release Summary

Vendor	Name *	Version *
<div>Click to set vendor</div>	<div>Test Component</div>	<div>Enter Version</div>
Programming Languages	Operating Systems	CPE ID
<div>e.g., Java,C++, C#,...</div>	<div>e.g.,Linux,MAC,Windows,...</div>	<div>Enter CPE ID</div>
Release Date	Licenses	Download URL
<div>Enter Release Date</div>	<div>Click to set Licenses</div>	<div>Enter URL</div>
Clearing State	Release Mainline State	Created on
<div>New</div>	<div>Open</div>	<div>2019/07/11</div>
Created by	Contributors	Moderators
<div>Will be set automatically</div>	<div>Click to edit</div>	<div>Click to edit</div>

SW360 | © Siemens AG 2013-2017, Bosch Software Innovations GmbH 2017 | [Report an issue](#) | Version: 3.4.0-SNAPSHOT | Branch: master (2fa916d) | Build time: 2019-07-11T07:47:11Z

# Register project Information

Create Project Information which include Component information  
[Projects]-[Add Project]

New Project

Summary

Administration

Linked Releases And Projects

General

Name \*

Enter Name

Version

Enter Version

Project visibility \*

Group and Moderators

Created by

Will be set automatically

HomePage URL

Enter Home Url

Wiki URL

Enter Wiki Url

Project type \*

Customer Project

Tag

Enter one word tag

Description

Enter Description

☐ Enable Security Vulnerability Monitoring

☐ Enable Displaying Vulnerabilities

Roles

Group \*

test org

Project manager

Click to edit

Project owner

Click to edit

SW360 | © Siemens AG 2013-2017, Bosch Software Innovations GmbH 2017 | [Report an issue](#) | Version: 3.4.0-SNAPSHOT | Branch: master (2fa916d) | Build time: 2019-07-11T07:47:11Z

# Create License Document

[Projects]-[Linked Releases And Projects]-[Generate License Info]

[Home](#) [Projects](#) [Components](#) [Licenses](#) [ECC](#) [Vulnerabilities](#) [Moderation](#) [Search](#) [Admin](#) [Preferences](#)

[Projects](#) / [Vim\\_test\\_project](#)

Project: [Vim\\_test\\_project](#) [Edit](#)

[Summary](#)  
[Administration](#)  
[Linked Releases And Projects](#)  
[Linked Releases Hierarchy](#)  
[Attachment Usages](#)  
[Clearing Status](#)  
[ECC Status](#)  
[Attachments](#)  
[Vulnerabilities](#) 34 / 34

Linked Releases And Projects

Name	Project state	Relation	Type	Clearing State	Main Licenses
<a href="#">bash 4.3-11+deb8u2</a>		Unknown	OSS	New	
<a href="#">Vim_test 2.7</a>		Unknown	OSS	New	

Projects only

[Export Spreadsheet](#) [Generate License Info](#) [Generate Source Code Bundle](#)

SW360 | © Siemens AG 2013-2017, Bosch Software Innovations GmbH 2017 | [Report an issue](#) | Version: 3.4.0-SNAPSHOT | Branch: master (cb4ad86) | Build time: 2019-06-13T10:46:34Z



# Confirm Vulnerabilities

## Check OSS Vulnerabilities [Components]-[Vulnerabilities]

SW360 ▶

Home

Projects

Components

Licenses

ECC

Vulnerabilities

Moderation

Search

Admin ▾

Preferences

Components

 / Test Component

Component: Test Component

MergeEditSubscribe

Summary

Release Overview

Attachments

Vulnerabilities 1 + 0

Showing 200 latest vulnerabilities out of 1 in total.

Show 10 entries

Search:

Release	External id	Priority	Title	Matched by	Verification	Action
<input type="checkbox"/> Test Component 1.0	CVE-2013-0253	🚫	CVE-2013-0253	CPE	Checked	

Showing 1 to 1 of 1 entries

Change verification state of selected vulnerabilities to Not Checked

Apply

• 1 of the vulnerabilities were matched by CPE

Print

Select all

Select none

Previous

1

Next

SW360 | © Siemens AG 2013-2017, Bosch Software Innovations GmbH 2017 | Report an issue. | Version: 3.4.0-SNAPSHOT | Branch: master (2fa916d) | Build time: 2019-07-11T07:47:11Z

Q & A

[kouki1.hama@toshiba.co.jp](mailto:kouki1.hama@toshiba.co.jp)

Thank You